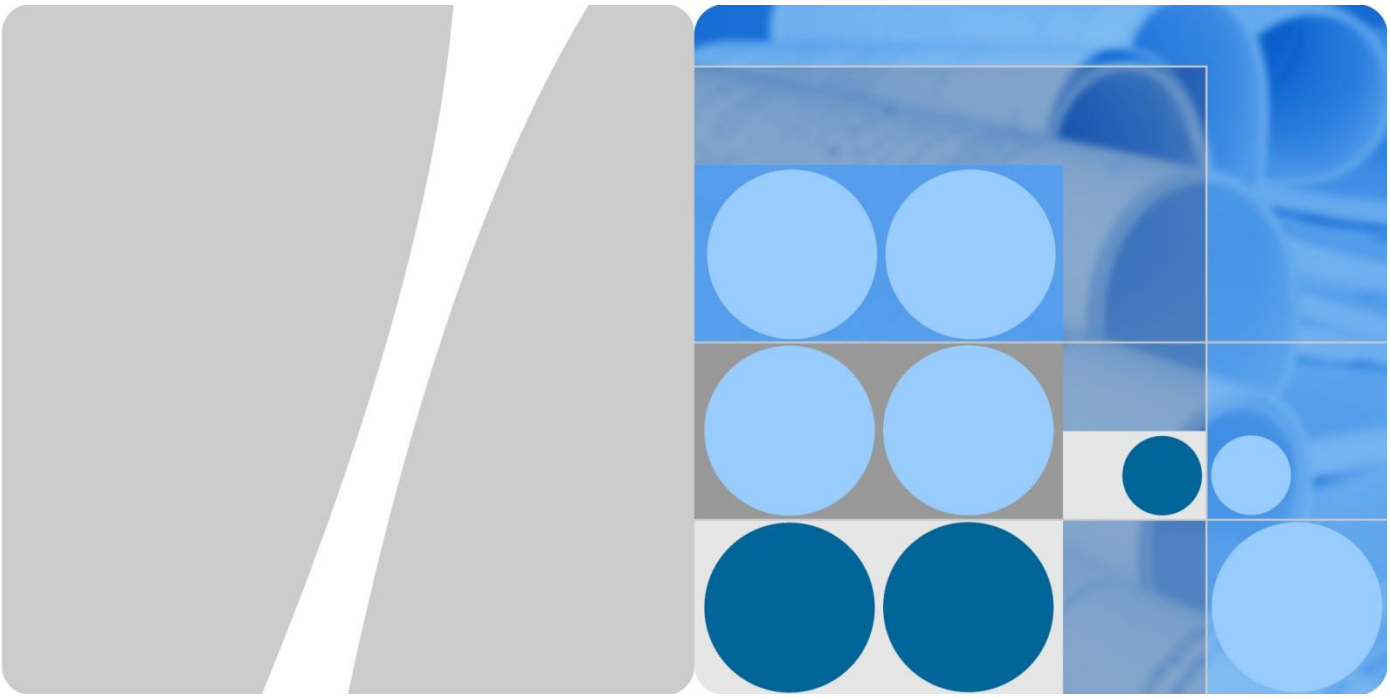


WLAN Hotspot2.0 Technology Whitepaper

Issue 1.0

Date 2015-06-18

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Keyword

WLAN, 802.11u, Hotspot2.0

Abstract

Wi-Fi has been widely used. Almost all smart terminals support this function. However, there are many usability issues in today's Wi-Fi hotspots. Users have to enable the Wi-Fi function to search for networks, select networks based on SSIDs, and enter their user names and passwords to connect to networks. More convenient Wi-Fi networks that are similar to cellular networks are imperative. Therefore, Wi-Fi Alliance (WFA) develops the Hotspot 2.0 standard to meet the demand. Huawei WLAN products support the Hotspot 2.0 feature. This document describes the technical principles of Hotspot 2.0 and how to deploy Hotspot 2.0.

Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
HS2.0	Hotspot 2.0
NGH	Next Generation Hotspot
UE	User Equipment
ANQP	Access Network Query Protocol
ASRA	additional step required for access
GAS	generic advertisement service
HESSID	homogenous extended service set identifier
NAI	network access identifier
OI	organization identifier
NDS	Network Discovery and Selection
RSN	Robust Security Network
SSID	Service Set Identifier

Acronym and Abbreviation	Full Name
SSP	Subscription Service Provider
UI	User Interface
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance
WISP	Wireless Internet Service Provider
WISPr	Wireless Internet Service Provider Roaming

Contents

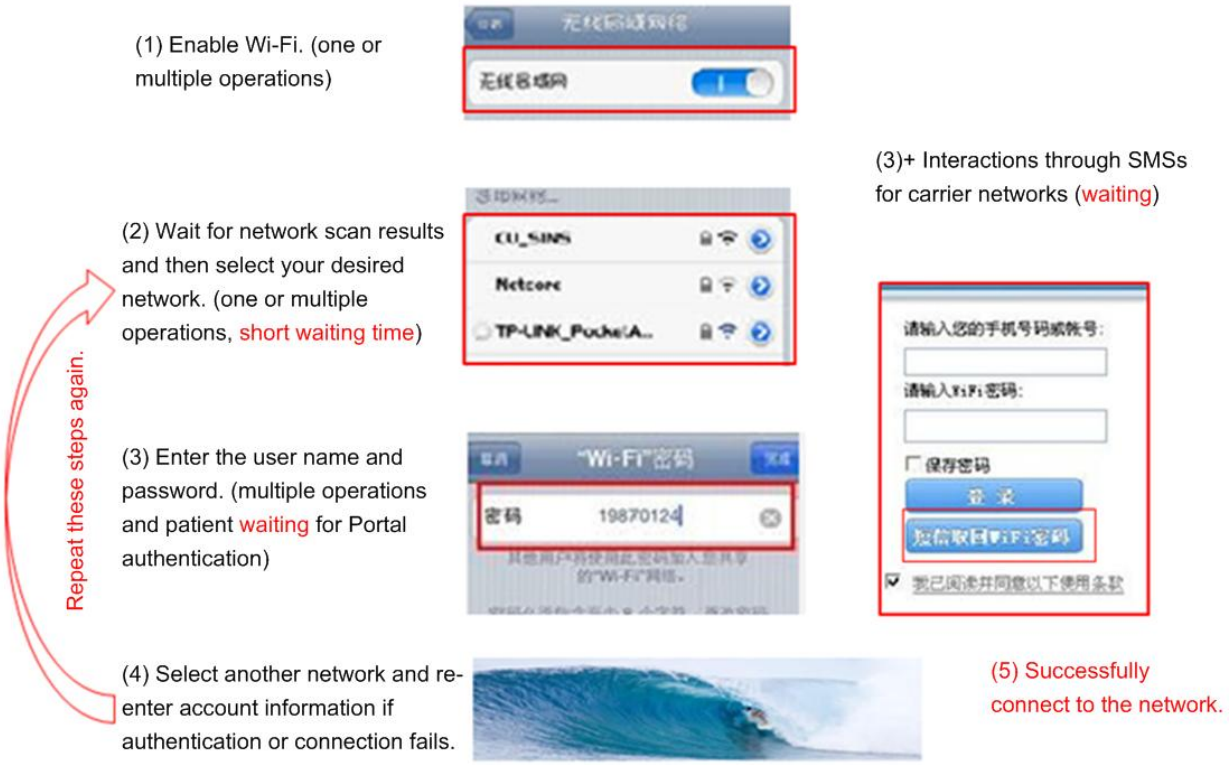
Figure

1 Overview

1.1 Background

Compared with cellular networks, Wi-Fi networks are inconvenient. User intervention is required. Users have to enable the Wi-Fi function to search for networks, select networks based on SSIDs, and enter their user names and passwords to connect to networks. Even if users have performed the preceding operations, they may not connect to networks successfully and use networks.

Figure 1-1 Typical Wi-Fi network access



In contrast, cellular network users only need to insert their SIMs to mobile phones that will then automatically connect to cellular networks. Then, users can make calls.

Devices connect to cellular networks automatically.

Automatic network selection and connection anywhere, anytime

Wi-Fi networks are capable of offering users a cellular-like experience, but there is no certification standard to streamline Wi-Fi network access and promote Wi-Fi in the market.

In the future, more and more smart phones will be used and almost all smart phones support the Wi-Fi function. It is necessary that Wi-Fi networks can provide the ease-of-use feature experienced on cellular networks. Therefore, Wi-Fi Alliance develops the Hotspot 2.0 standard to meet the demand.

In 2010, industry leaders formed the Hotspot 2.0 Task Group in the Wi-Fi Alliance. The goal was to rally the industry around a common set of standards that would minimize user intervention and offload data from cellular networks of carriers. Wi-Fi Alliance developed the Passpoint certification specification based on the Hotspot 2.0 technology to certify Wi-Fi hotspot products.

1.2 802.11u, HS2.0 and Passpoint

Figure 1-2 802.11u, HS2.0 and Passpoint

- 802.11u is a standard developed by IEEE.
- Hotspot 2.0 (HS2.0) is a specification developed by WFA based on IEEE 802.11u.
- Passpoint is the certification program launched by WFA. Passpoint-certified products support HS2.0.

1.3 Protocol Evolution

The following table describes Wi-Fi interoperability development phases:

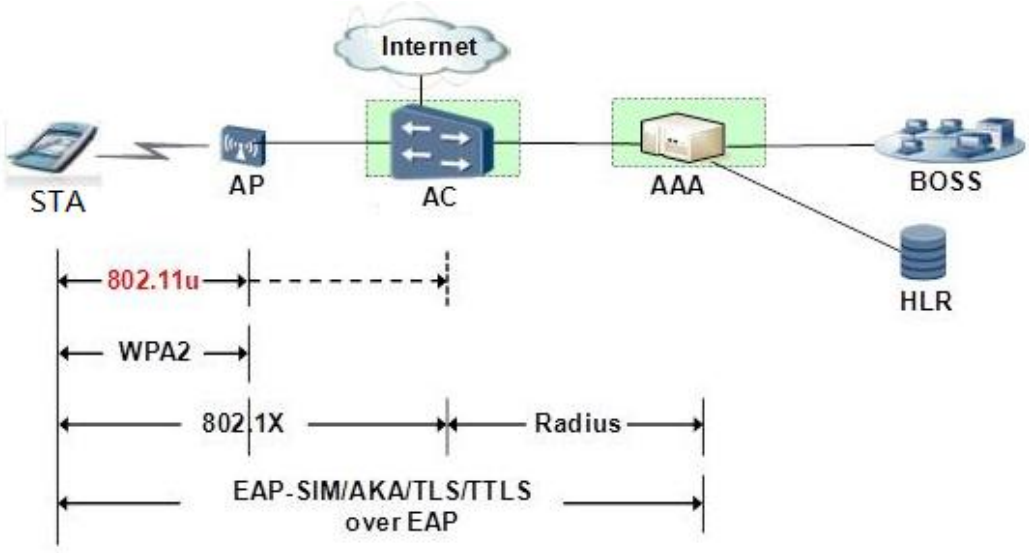
Organization	Proposal and Protocol	Description
IEEE	802.11u	IEEE released 802.11u in February 2011. 802.11u defines functions and procedures helping STAs discover and select proper APs automatically and interfaces interworking with external networks. Corresponding software configurations are required on APs and STAs.
Wi-Fi Alliance	Hotspot 2.0	Hotspot 2.0 enhances network discovery to make Wi-Fi networks as easy to use as cellular networks. Wi-Fi Alliance can certify Hotspot 2.0-capable devices. Hotspot 2.0 is built upon IEEE 802.11u, but it extends IEEE 802.11u. Hotspot 2.0 supports SIM and non-SIM devices and uses the 802.1X authentication. Hotspot 2.0 Release 1 has been published and Release 2 is in the draft state.
Wireless Broadband Alliance (WBA)	Next Generation Hotspot (NGH)	It is a commercial framework to provide better interworking. It is extended based on Hotspot2.0 and IEEE 802.11u.

2 Implementation of Hotspot 2.0

2.1 HS2.0 Solution Overview

A HS2.0 network consists the following network elements (NEs):

Figure 2-1 Typical HS2.0 network



The functions or tasks of these NEs are as follows:

- Network discovery and selection (802.11u): AP, and UE
- Rogue AP avoidance, wireless privacy, and encryption over the air interface (WPA2+802.1x): AP, AC/BRAS, and UE
- User authentication (EAP-SIM/AKA, EAP-TLS, and EAP-TTLS): AAA and UE

Hotspot 2.0 is built on the following three key technologies:

- IEEE 802.11u

  IEEE 802.11u enables STAs and APs to exchange the following information prior to association: hotspots, network information, operation information, service providers, heterogeneous system information, roaming subscription, policies, and authentication

information. Therefore, automatic network discovery, selection, and roaming can be implemented.

- WPA2/EAP

  WPA2 adopts EAP-TTLS, EAP-TLS, EAP-AKA, EAP-PSK, and other authentication methods to authenticate STAs based upon SIMs, USIMs, certificates, or keys, complementing SIM-based authentication on cellular networks.

- Online Sign-up and Policy Provisioning (Release 2)

  Online sign-up and policy provisioning are introduced.

Comparison of network configurations on Hotspot 2.0 and legacy networks

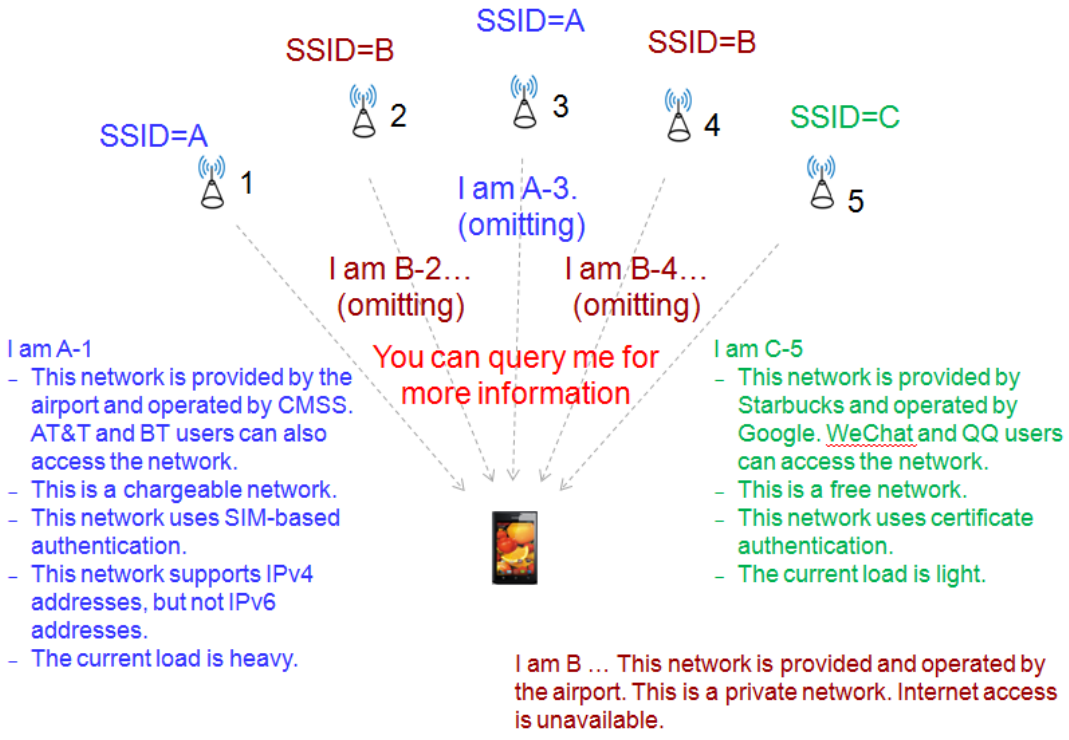
Item	Legacy	Hotspot2.0
Network discovery and selection	SSID	802.11u
Layer 2 authentication	None	802.1x
Layer 2 air encryption	None	802.11i
Layer 3 authentication	WebAuth WISPr1.0/2.0	EAP-SIM, EAP-AKA, EAP-TLS, and EAP-TTLS
HS Network	Untrusted	Trusted
Roaming	Manual	Yes (automatic)

2.2 Fundamentals of HS2.0

- IEEE 802.11u was proposed in 2004 and published in February 2011. This standard is used to implement interoperability between heterogeneous systems.
- IEEE 802.11u enables STAs and APs to exchange information prior to association. With the Generic Advertisement Service (GAS), APs can advertise more information and STAs use the information received from APs or further query the following information by using the Access Network Query Protocol (ANQP): hotspots, network information, operation information, service providers, heterogeneous system information, roaming subscription, policies, and authentication information.

  This protocol realizes automatic network discovery, selection, and roaming at hotspots.

Figure 2-2 Automatic network discovery in HS2.0



In short, STAs can obtain network information before associating with WLANs so that STAs can automatically select networks.

2.2.1 GAS

To communicate with external networks, Wi-Fi terminals need communication channels. GAS defined in IEEE 802.11u for 802.1 networks provides a frame exchange process (Request/Response). IEEE 802.11u only defines the GAS for 802.11 networks.

The GAS allows STAs to obtain pre-association information before associating with APs so that they can select suitable networks.

2.2.2 ANQP

GAS frames are used to transport the ANQP. ANQP uses the GAS Request/Response mechanism to obtain subscription service provider network (SSPN) information. The Media Independent Handover (MIH) is a protocol similar to the ANQP. HS2.0 is built upon the ANQP protocol.

GAS is a framework that provides transport for advertisement services like ANQP. MIH and Emergency Alert System (EAS) are similar to ANQP, but HS2.0 uses ANQP.

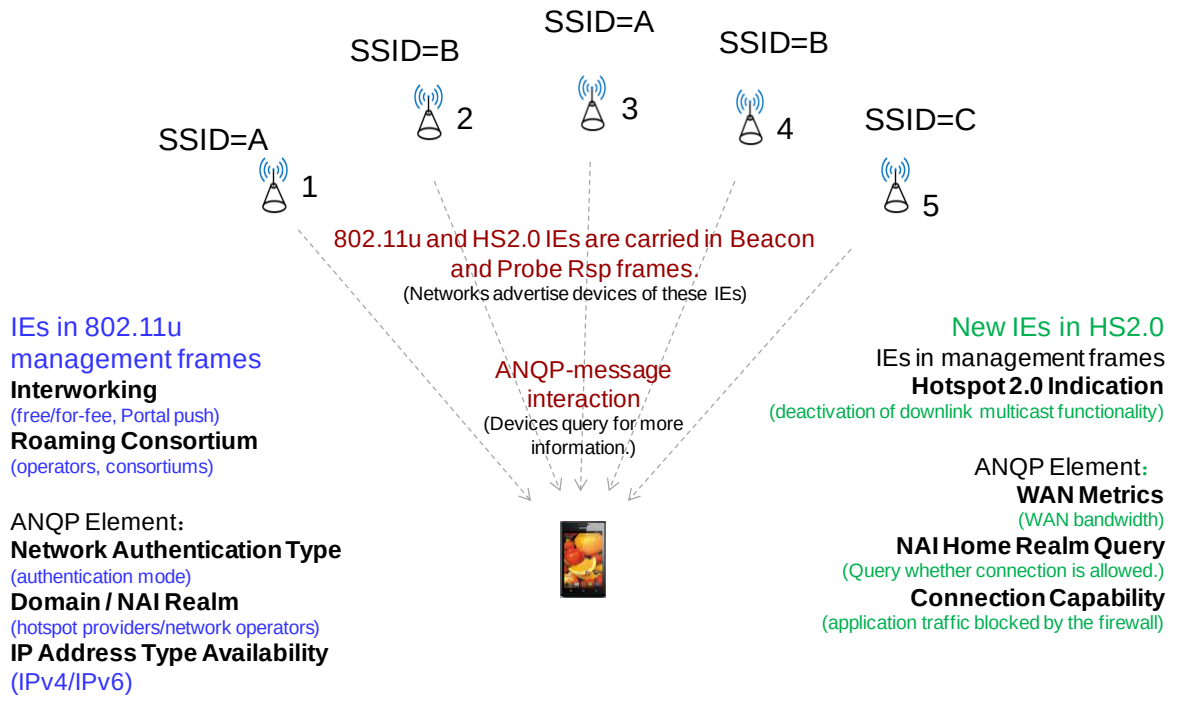
2.3 Network Discovery and Selection

IEEE 802.11u defines a mechanism that allows STAs to obtain WLAN network information. With this mechanism, an AP notifies STAs of WLAN information by sending Beacon or Probe Response frames or through GAS. WLAN information includes lists of home service providers and roaming partners, supported authentication types, AP traffic load, and the number of online users. Based on the received WLAN information, the STAs select the best WLAN network to access, where the STAs will be automatically authenticated.

2.3.1 Extension of Air-interface Frames and Protocols

To enable STAs to obtain network information for them to select a network before they associate with a WLAN, IEEE 802.11u and HS2.0 extend air-interface frames to advertise network information prior to association.

Figure 2-3 How automatic network discovery in HS2.0 is implemented



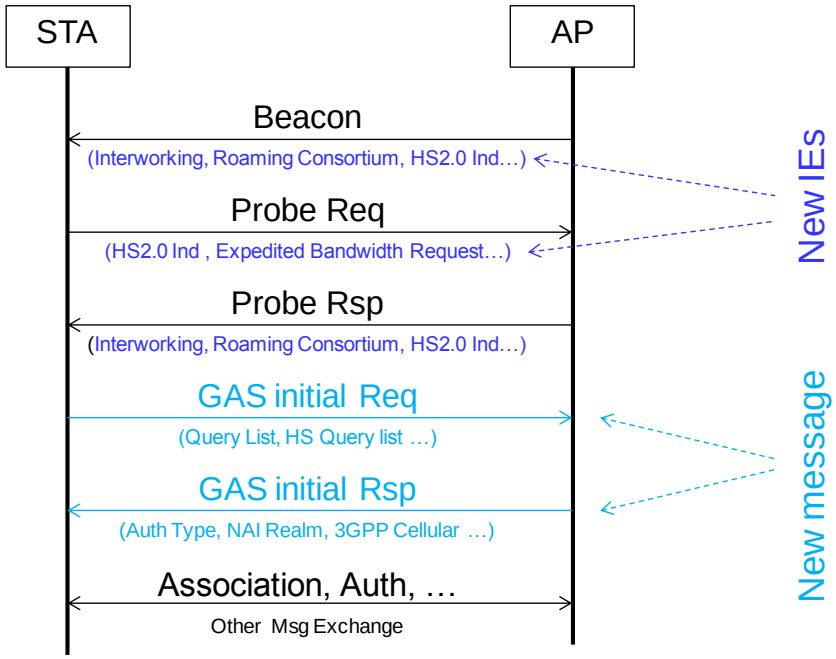
Note: HS2.0 is built on IEEE 802.11u.

STAs can connect to networks automatically if they recognize any of the items contained in the following advertisement messages and meet requirements of the corresponding EAP method:

- NAI realm list, domain list, cellular PLMN, and roaming consortium list

  If the information in advertisement messages is insufficient, STAs can send NAI Home Realm Query elements through ANQP to inform networks of their home realms. The networks then check the realms and respond to STAs. Figure 2-4 shows how air interface messages are exchanged.

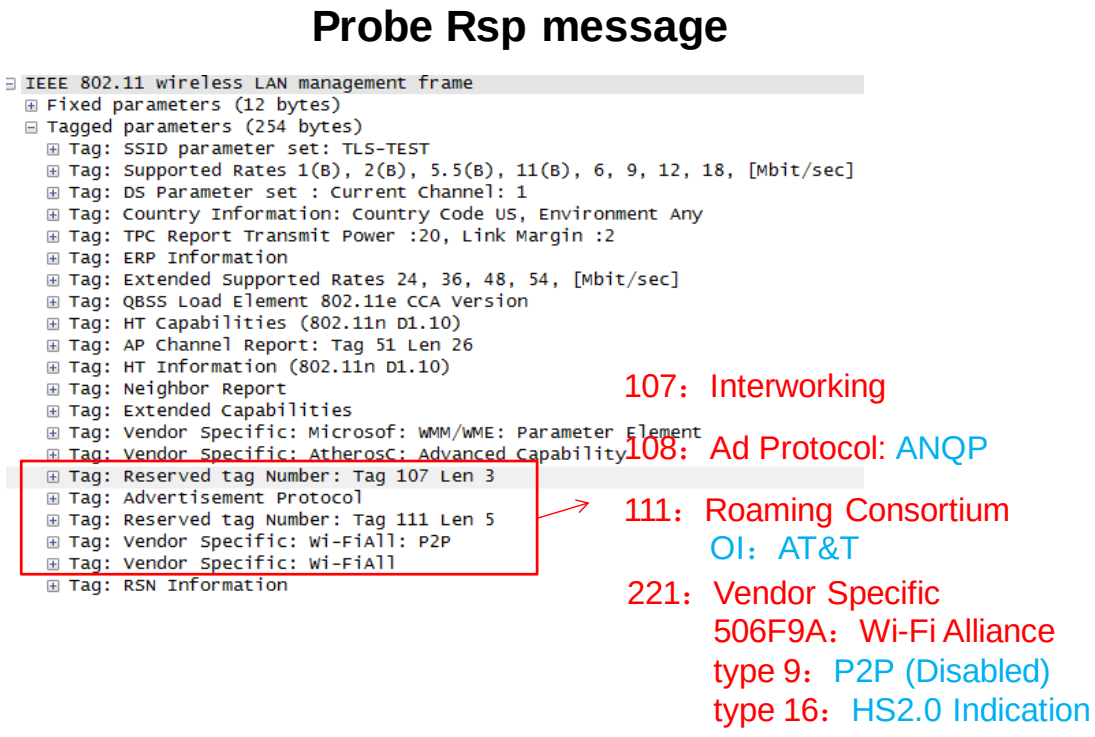
Figure 2-4 Air-interface message interaction in HS2.0



Note: Message interactions marked in black are traditional message interactions.

Figure 2-5 analyzes captured packets of Probe Rsp messages.

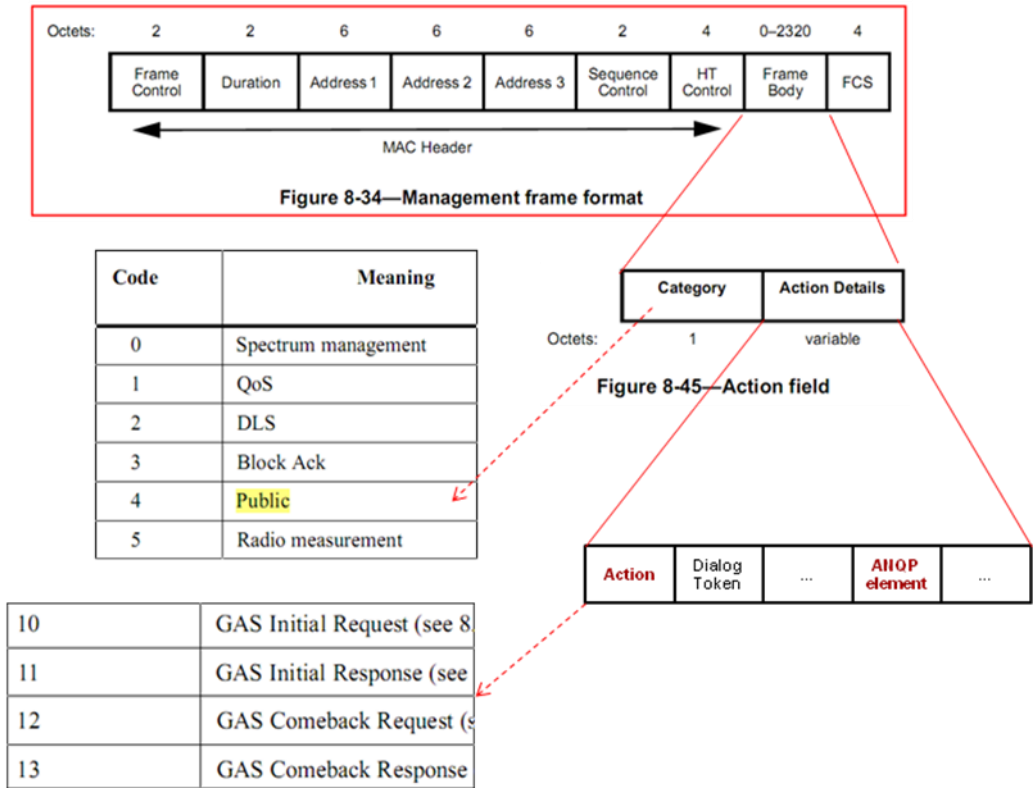
Figure 2-5 Analysis of captured packets of Probe Response messages



Because the Wireshark tool is an earlier version, not all HS2.0-related information elements (IEs) are parsed in the preceding figure.

Figure 2-6 shows the packet format of GAS messages.

Figure 2-6 802.11u GAS packet format



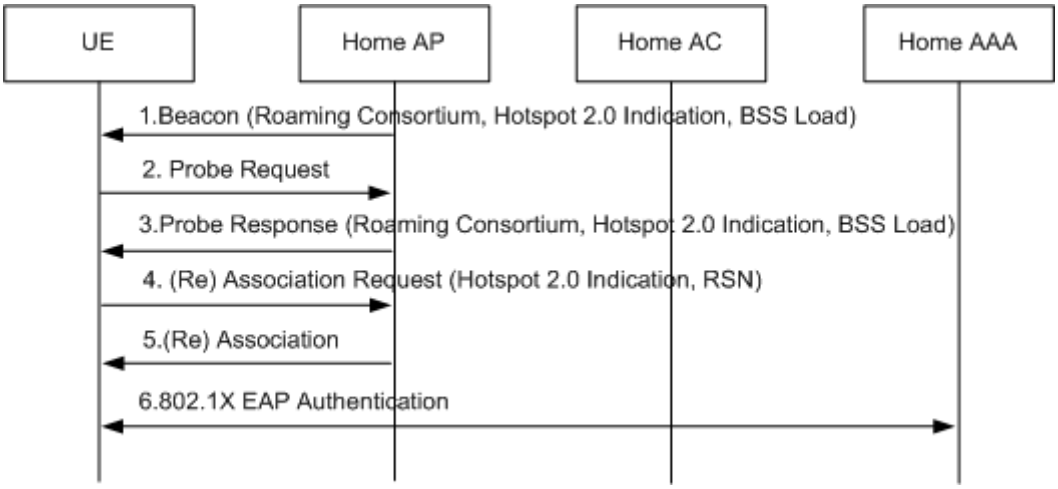
2.3.2 Home Network Discovery and Selection

STAs obtain WLAN information by using two procedures: home network discovery and selection, and visited network discovery and selection.

Users have been registered with their home service provider and have been configured with a USIM/SIM, credential, user name and password, and organization identifier (OI) of the home service provider.

Figure 2-7 shows the procedure for home network discovery and selection when a UE accesses the home WLAN network for the first time.

Figure 2-7 Home network discovery and selection process



Process Description

1. The UE performs a passive scan. That is, the UE waits for a Beacon frame from the home AP. The Beacon frame contains information that includes the Hotspot 2.0 Indication, basic service set (BSS) load, Internet connectivity flag, charging flag, and information about one to three service providers.
2. The UE performs an active scan. That is, the UE sends to the home AP a Probe Request frame with the Access Network Type field specified to indicate the desired access network type. The Access Network Type field can be set to "Private network" or "Chargeable Public Network."
3. Upon receiving the Probe Request frame, the home AP compares the value of the Access Network Type with the network type configured on the home AP, the home AP responds with a Probe Response frame, which includes information elements (IEs) similar to those in the Beacon frame. If the Probe Request frame does not contain the Access Network Type field, the home AP does not check this field.
4. The UE either receives a Beacon or Probe Response frame from one AP, or multiple Beacon or Probe Response frames from multiple APs.

   A HS2.0-capable UE checks whether the received Beacon or Probe Response frame carries the Hotspot 2.0 Indication element. In this way, the UE determines whether a home AP supports HS2.0. (An AP supporting HS2.0 supports the 802.11u standard, WPA2, and 802.1X EAP authentication.) If the home AP supports HS2.0, the UE parses the Roaming Consortium element included in the received Beacon or Probe Response frame and obtains the OI of the WLAN service provider. By doing so, the UE determines whether it is allowed to access the WLAN network. Before the access, the UE learns WLAN network load based on the BSS Load element included in the received Beacon or Probe Response frame. Then the UE selects a lightly loaded hotspot to which it will access.

   Traditional UEs that do not support HS2.0 cannot recognize the fields related to HS2.0. With such UEs, users need to manually select a WLAN network.

   Upon determining a target WLAN network, the UE sends an Association Request frame to the home AP. The Association Request frame includes the HS2.0 Indication IE, indicating that the UE supports HS2.0. This frame also includes the RSN IE, indicating that CCMP encryption and 802.1X authentication are used.
5. The home AP responds to the UE with an Association frame.

6. The UE starts the 802.1X authentication with the home AAA. Specifically, the UE reports to the home AAA the NAI field in the format of username@realm. Based on the route information provided by the NAI field, the home AAA connects to the authentication server of the home service provider for authentication on the UE.

2.3.3 Visited Network Discovery and Selection

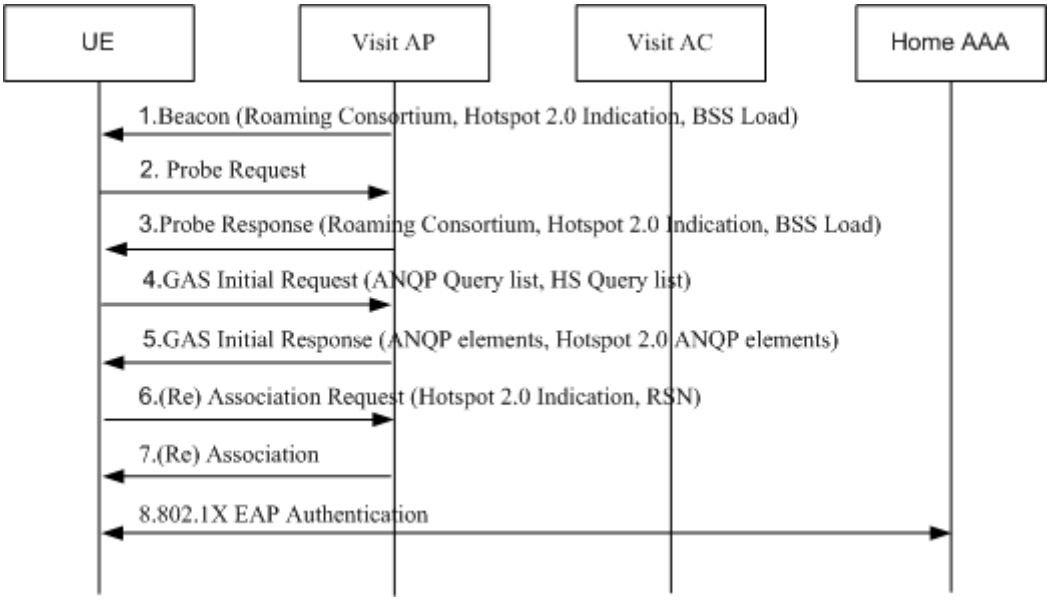
In the scenario where a HS2.0-capable UE accesses a visited WLAN, the visited WLAN must have roaming agreements with the home network. Additionally, some or all of the following information related to the home network and roaming consortium must be configured on the visited WLAN:

- Roaming Consortium List, including the operator OI or roaming consortium OI
- Public land mobile network (PLMN) contained in the 3GPP Cellular Network Information IE
- NAI Realm List, service provider list, domain name, and authentication type

Configure the preceding information as required.

Figure 2-8 shows the process for visited network discovery and selection.

Figure 2-8 Process for visited network discovery and selection



Process Description

1. Steps 1 through 3 are the same as steps 1 through 3 in section 2.3.2 "Home Network Discovery and Selection"
2. The UE either receives a Beacon or Probe Response frame from one AP, or multiple Beacon or Probe Response frames from multiple APs.

   A HS2.0-capable UE checks whether the received Beacon includes the HS2.0 Indication element. In this way, the UE determines whether a visit AP supports HS2.0. If the visit AP supports HS2.0, the UE parses the Advertisement Protocol element included in the received Beacon or Probe Response frame and obtains the advertisement protocol

supported on the WLAN network. By doing so, the UE selects an appropriate advertisement protocol to query WLAN network information based on its capability.

Traditional UEs that do not support Hotspot 2.0 cannot recognize the fields related to Hotspot 2.0. With such UEs, users need to manually select a WLAN network.

The UE sends a GAS Initial Request frame to the visit AP to obtain other WLAN network information, including a list of all available service providers, supported authentication types, hotspot operators, ports, and traffic over the WAN port. WAN stands for wide area network.

3. The visit AP responds to the UE with a GAS Initial Response frame. The GAS Initial Response frame includes corresponding ANQP elements based on the ANQP Query List and HS Query list elements included in the GAS Initial Response frame.
4. The UE either receives a GAS Initial Response frame from one AP, or multiple GAS Initial Response frames from multiple APs. The UE selects a WLAN network based on the obtained WLAN information (such as the domain name and authentication type), preset NAI, and access credential.

   Upon determining a target WLAN network, the UE sends an Association Request frame to the visit AP. The Association Request frame includes the HS2.0 Indication IE, indicating that the UE supports HS2.0. This frame also includes the RSN IE, indicating that CCMP encryption and 802.1X authentication are used.
5. The visit AP responds to the UE with an Association frame.
6. The UE starts the 802.1X authentication with the home AAA. Specifically, the UE reports to the home AAA the NAI field in the format of username@realm. Based on the route information provided by the NAI field, the home AAA connects to the authentication server of the home service provider for authentication on the UE.

2.4 Hotspot Selection Policies

If there are multiple accessible hotspots, how can a UE select a suitable hotspot? The hotspot selection policies are as follows:

If there are multiple CMCC hotspots, the UE can select the hotspot with the smallest load.

If both CMCC and Google hotspots are accessible, the UE can select the free hotspot.

The UE selects a suitable hotspot based on information contained in the following elements:

- BSS Load: Provides the number of terminals on the BSS and channel load.
- IP Address Type Availability Information: Provides information about the IP address version and type such as IPv4 and IPv6 and indicates whether network address translation (NAT) is allowed.
- WAN Metrics: Provides the WAN link status and downlink and uplink speed and load.
- Connection Capability: Provides information on the status of IP protocols and ports.

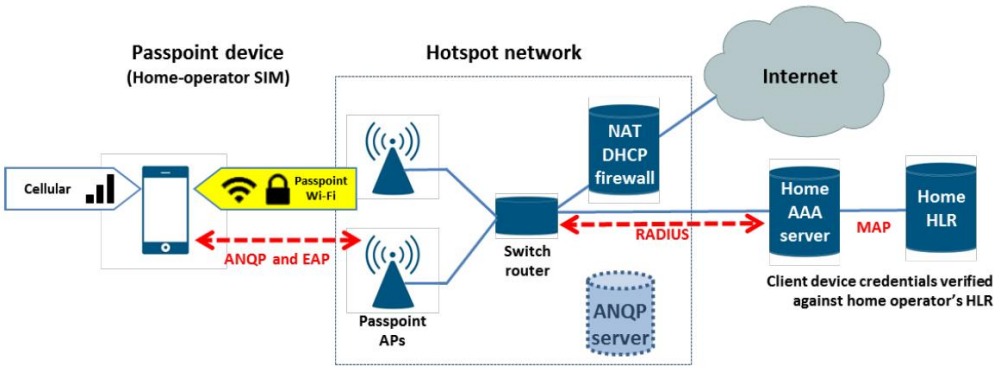
UEs implement hotspot algorithms to select the most suitable hotspot. This document will not discuss these algorithms in detail.

3 Hotspot2.0 Network Deployment

3.1 Hotspot2.0 Network Architecture

3.1.1 Hotspot 2.0 Network Deployment Based on Authentication Using Cellular Network Credentials

Figure 3-1 Passpoint hotspot deployment: SIM device

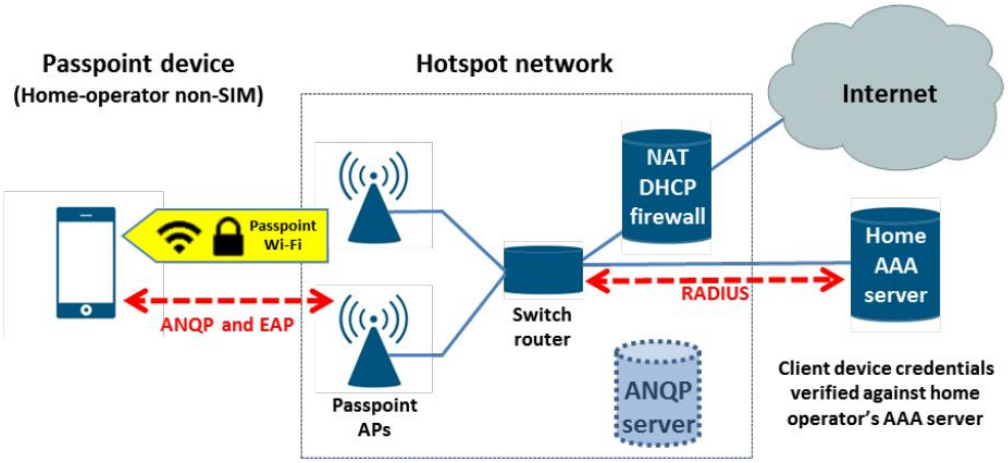


Network selection and authentication process:

1. The device detects the Hotspot 2.0 Indication IE in the Beacon frame sent by the AP.
2. The device queries ANQP server for 3rd Generation Partnership Project (3GPP) cellular network information and roaming consortium OIs.
3. The device compares the received information and OIs with its list of credentials and preferred networks.
4. The device automatically associates with Passpoint AP.
5. The device performs the 802.1x authentication with the home authentication, authorization and accounting (AAA) server using Extensible Authentication Protocol–Subscriber Identity Module (EAP-SIM), or EAP-Authentication and Key Agreement (EAP-AKA).
6. The home AAA server communicates with the core network device home location register (HLR) using the Mobile Application Part (MAP) to complete the authentication.

3.1.2 Hotspot 2.0 Network Deployment Based on Authentication Using Non-cellular Network Credentials

Figure 3-2 Passpoint hotspot deployment: non-SIM device



Network selection and authentication process:

1. The device detects the Hotspot 2.0 Indication IE in the Beacon frame sent by the AP.
2. The device queries ANQP server for network access identifier (NAI) realms and roaming consortium OIs.
3. The device compares the received realms and OIs with its list of credentials and preferred networks.
4. The device automatically associates with Passpoint AP.
5. The device performs the IEEE 802.1X authentication with the Home AAA server using EAP-Transport Layer Security (EAP-TLS) or EAP-Tunneled TLS (EAP-TTLS) with MS-CHAPv2.

3.2 Network Discovery and Selection

3.2.1 SP Identifier and Authentication Method

1. 3GPP cellular network information

   The 3GPP cellular network information is transported in ANQP elements and contains the cellular operator's PLMN ID. The PLMN ID consists of the mobile country code (MCC) and mobile network code (MNC) elements.

   A mobile device with SIM or USIM credentials transmits a GAS/ANQP query for 3GPP cellular network information, and compares the response with the PLMD ID stored on its SIM or USIM to determine whether the home cellular SP's network can be accessed through the Passpoint AP. The mobile device knows the EAP method (EAP-SIM or EAP-AKA) required to authenticate with its Home service provider (SP), and automatically uses it.
2. NAI Realm List

The NAI Realm List element provides a list of NAI realms corresponding to SPs that can authenticate a mobile device using user name/password or certificate credentials.

The EAP-TTLS is the authentication using certificate credentials and EAP-TTLS with MS-CHAPv2 is the authentication using user name/password credentials. An SP may support multiple authentication methods, but mobile devices can automatically select a correct authentication method.

Hotspot operators can configure the NAI Realm List as follows:

- The realms of all the roaming partners accessible at the Passpoint AP are added to this list.
- A realm corresponding to a 3GPP PLMN ID may also be added to the NAI Realm List.
- When a device has been provided with credentials by the SP providing the service, the device does not need to use the information contained in the EAP method list portion of the NAI Realm List.
- The EAP method list may be configured to support devices that do not know what EAP methods are used by a given SP.

A device compares the NAI Realm List with the realm information stored in the device to determine the access policy.

3. Roaming Consortium List

   The Roaming Consortium List provides a list of OIs of roaming consortium and SPs that are roaming partners of the hotspot service provider and that are accessible from the Passpoint AP. The roaming consortium or a single SP is identified by OI values. This list does not provide information on authentication methods. The mobile device may obtain OI information first, and then implement a full NAI GAS/ANQP query to obtain the full realm name and required EAP method.

3.2.2 Hotspot Identification

1. Domain Name List

   The domain name is the identifier of an entity operating the hotspot network. A Hotspot operator might use more than one domain name to identify itself. For example, the domain names wlan.mnc410.mcc310.3gppnetwork.org, att.com, and attwireless.com all indicate the same SP, AT&T.

   The mobile device compares the fully qualified domain name (FQDN) of an SP that is contained in a domain name to determine whether a hotspot is operated by its Home SP. For example, starbucks.att.com and mcdonalds.att.com are operated by the same SP, att.com. Access of AT&T users to these two hotspots is not roaming access.

   If the SP's name is in the realm list but not in the domain name list, a mobile device choosing that SP will be considered to be roaming.

2. Venue Name Information

   This element provides the hotspot location information. Hotspot Operators can use multiple languages to list venue names to assist users during manual hotspot selection.

3. Venue Info Field

   This element provides information about the group and type of hotspot venues to assist users during manual hotspot selection. The group and type descriptors are drawn from the International Building Code.

4. Operator's Friendly Name

This element provides the friendly name of the Hotspot Operator to assist users during manual hotspot selection. Operator friendly names can be expressed in multiple languages.

3.2.3 Network Parameters

1. IP Address Type Availability Information

   This element provides information about the IP address version and type that are used by the hotspot operator and that would be allocated to a mobile device after it authenticates to the network.

2. WAN Metrics

   This element provides information about the load on the WAN link.

   The range for the load measurement duration (LMD) is recommended to set to 1 to 15 minutes.

3. Connection Capability

   This element provides information about communication protocols and ports used in the hotspot.

4. Operating Class Indication

   This element provides information about the channels and frequency bands used by the APs in a venue having the same SSID.

5. Network Authentication Type Information

   This element is not used in Hotspot 2.0 Release 1 and no additional step required for access (ASRA) is indicated. Therefore, this element is not configurable.

3.2.4 Capability Query

1. HS Query List
2. HS Capability List
3. NAI Home Realm Query

   This element can shorten the realm list transmitted over air interfaces.

3.2.5 Other Beacon Elements

- HESSID Information Element

  SSID is not a globally unique identifier. The homogeneous extended service set identifier (HESSID), a globally unique identifier, overcomes this shortcoming.

  The HESSID is used to identify a group of APs connected to the same SP.

  The HESSID is a MAC address. It is the same as the value of the basic service set identifier (BSSID) of one of the APs on the network.

- Access Network Type Field

  The access network type field provides network type information, for example, private network or public network.

- Internet Available Field

  The Internet available field indicates whether Internet access is available at a hotspot.

- BSS Load Information Element

  This element provides BSS load information.

3.3 Security Features

3.3.1 WPA2-Enterprise

HS2.0 uses the WPA2-Enterprise security policy other than P2P, DLS, TDLS, WPA2-PSK, TKIP, and WEP.

The following table lists the relationships between credential types and EAP methods.

Credential Type	EAP Method
Certificate	EAP-TLS
SIM	EAP-SIM
USIM	EAP-AKA
Username/password (with server-side certificates)	EAP-TTLS with MS-CHAPv2

3.3.2 Layer 2 Filtering

Layer 2 filtering must be enabled on Passpoint APs functioning as "free public network" or "chargeable public network".

The firewall function can be enabled either on a Passpoint AP or on an external entity to which the AP is connected.

The proxy Address Resolution Protocol (ARP) service should be enabled.

3.3.3 Disabling the Broadcast/Multicast Capability

It is recommended that hotspots using Passpoint APs disable the multicast/broadcast capability.

No GTKs are used.

It is recommended that proxy-ARP service be used no matter the broadcast/multicast functionality is disabled or enabled.

3.4 Terminal Compatibility

When you deploy HS2.0 APs, you can use original SSIDs of non-HS2.0 APs.

HS2.0 APs support legacy terminals that do not support HS2.0, but employ WPA2-Enterprise security. HS2.0 APs do not provide the full backward compatibility.

4 Appendix

4.1 Wi-Fi CERTIFIED Passpoint

Wi-Fi CERTIFIED Passpoint was launched in 2012 as an industry-wide solution to streamline network access in hotspots and eliminate the need of network search and identity authentication for users each time they connect. On Wi-Fi networks that do not support Passpoint, users must search for and choose a network, request the connection to the AP each time, and in many cases, must re-enter their authentication credentials. Passpoint automates the entire process, enabling a seamless connection between hotspot networks and mobile devices, all while delivering the highest WPA2 security.

Passpoint was jointly developed by Wi-Fi Alliance, mobile device manufacturers, network equipment vendors, and operators. Passpoint is a great solution for end users, network operators, and device vendors. In addition to providing a reliable, secure, in-pocket connection experience in Wi-Fi hotspots, Passpoint is delivering values to service providers in the following ways:

- Supports data offload with instant network detection, selection, and authentication.
- Increases customer satisfaction and reduces customer churn.
- Offers best-in-class security for SIM and non-SIM devices alike.

Passpoint is a foundational ingredient to Wi-Fi roaming standards currently taking shape across the world. Multi-operator trials on Passpoint-certified equipment, as part of the Next Generation Hotspot program, are taking place now. Wi-Fi Alliance is collaborating with various industry groups to ensure the building blocks are in place to create a truly global Wi-Fi roaming experience.

4.2 Reference Standards and Protocols

1. IEEE 802.11u: *IEEE802.11u-2011*
2. Hotspot 2.0 Release 1: *Hotspot 2.0 (Release 1) 5 Technical Specification Version 1.0.0*