

White Paper

Wi-Fi Direct™

1.0 EXECUTIVE SUMMARY

Wi-Fi Direct is a new technology defined by the Wi-Fi Alliance wherein capable devices can connect directly to each other quickly, securely and conveniently to do tasks such as printing, synchronization, and sharing of data. In this paper we provide a thorough overview of the functionalities defined in Wi-Fi Direct Specification along with details of the underlying protocol.

This paper provides an overview of the Wi-Fi Direct specification, focusing on its novel functionalities and illustrating three representative group formation procedures along with power saving mechanisms involved.

CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 EXECUTIVE SUMMARY	1
2.0 INTRODUCTION	2
3.0 TECHNICAL OVERVIEW	2
3.1 ARCHITECTURE	2
3.2 GROUP FORMATION	3
3.3 SERVICE DISCOVERY	6
3.4 WFD STATE MACHINE.....	7
3.5 SECURITY	7
3.6 POWER SAVING	8
4.0 PACKET ANALYSIS.....	10
5.0 TESTING TECHNIQUES	14
6.0 REFERENCES	15

2.0 INTRODUCTION

More than a decade after its initial design, the IEEE 802.11 standard [1], has become one of the most common ways to access the Internet. Wi-Fi has its presence in many kinds of devices like smart-phones, TV, printers, automobiles, healthcare etc. For long wi-fi was limited to basic model of Access Points creating wireless network and Station devices connecting to wireless networks. Wi-Fi Direct allows devices to communicate directly with each other using methods similar to traditional Wi-Fi, except without requiring the use of a central access point. Instead, the devices use a *"Software Access Point"* (Soft AP). Direct device to device connectivity was already possible in the original IEEE 802.11 standard by means of the ad-hoc mode of operation. However this never was able to mark its presence in the market due to several drawbacks or limitations in the requirements, e.g. lack of efficient power saving support or extended QoS capabilities [2]. Latest advancement related to in the Wi-Fi device to device communications space is 802.11z, also known as *Tunneled Direct Link Setup* (TDLS), which enables direct device to device communication but requires stations to be associated with the same AP.

Wi-Fi Direct technology as described in *"Wi-Fi Peer-to-Peer (P2P) Technical Specification"* takes a different approach, to enhance device to device connectivity. Instead of leveraging the ad-hoc mode of operation, Wi-Fi Direct builds upon the successful IEEE 802.11 infrastructure mode and lets devices negotiate who will take over the AP-like functionalities. Thus, enables legacy Wi-Fi devices to connect to the Wi-Fi Direct network that may have not been possible otherwise.

3.0 TECHNICAL OVERVIEW

In a typical Wi-Fi network, client scans and associate to wireless networks available, which are created and announced by Access Points (AP). Each of these devices has roles involving a different set of functionality. A major novelty of Wi-Fi Direct is that these roles are specified as dynamic, and hence a Wi-Fi Direct device has to implement both the role of a client and the role of an AP (sometimes referred to as Soft AP). These roles are therefore logical roles that could even be executed simultaneously by the same device, this type of operation is called Concurrent mode.

In order to establish a communication, P2P devices have to agree on the role that each device will assume at the time of negotiation. In the following we describe how this communication is configured using specified procedures, namely device discovery, role negotiation, service discovery, security provisioning and power saving.

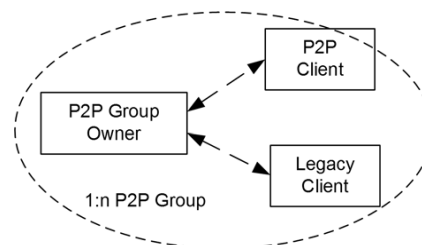
3.1 Architecture

Wi-Fi Direct devices, formally known as P2P Devices, communicate by establishing P2P Groups, which are functionally equivalent to traditional Wi-Fi infrastructure networks. The device implementing AP like functionality in the P2P Group is referred to as the P2P Group Owner (P2P GO), and devices acting as clients are known as P2P Clients.

This GO and client functionality is dynamic and is negotiated at the time of initial network setup. Two P2P devices discover each other; they negotiate their roles (P2P Client and P2P GO) to establish a P2P Group. Once the P2P Group is established, other P2P Clients can join the group as in a traditional Wi-Fi network. Legacy clients can also communicate with the P2P GO, as long as they support the required security mechanisms. By default Wi-Fi Direct uses WPA2PSK as security standard. In this way, legacy

devices do not formally belong to the P2P Group and do not support the enhanced functionalities defined in Wi-Fi Direct, but they simply “see” the P2P GO as a traditional AP.

The logical nature of the P2P roles supports different architectural deployments; one of this is illustrated in Fig 1 represents a scenario with two P2P groups. The first scenario is a mobile phone sharing its 3G connection with two laptops; in this first scenario, the three devices form a group, the phone is acting as P2P GO while the two laptops behave as P2P Clients. In order to extend the network, one of the laptops establishes a second P2P Group with a printer; for this second group, the laptop acts as P2P GO. In order to act both as P2P Client and as P2P GO the laptop will typically alternate between the two roles by time-sharing the Wi-Fi interface.



P2P components and topology

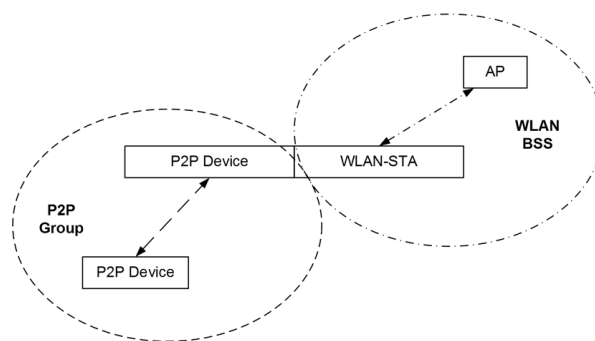


Fig.1 Wi-Fi Direct supported topologies

Source: P2P Technical Specification

Like a traditional AP, a P2P GO announces itself through *beacons* containing additional P2P Information Element. P2P IE is included in all management frames. Legacy devices ignore these information elements and action frames. The Wi-Fi Direct Specification requires that the P2P device which becomes the group owner should also provide the *DHCP* server application in their system [3] to provide P2P Clients with IP addresses. In addition, only the P2P GO is allowed to cross-connect the devices in its P2P Group to an external network. Finally, Wi-Fi Direct does not allow transferring the role of P2P GO within a P2P Group. In this way, if the P2P GO leaves the P2P Group then the group is torn down, and has to be re-established using some of the specified procedures.

3.2 Group Formation

There are several ways in which two devices can establish a P2P Group. Three types of group formation techniques are Standard, Autonomous and Persistent cases. An example of group formation case is illustrated in Fig 2.

Group Formation procedure involves two phases-

- Determination of P2P Group owner
 - Negotiated - Two P2P devices negotiate for P2P group owner based on desire/capabilities to be a P2P GO.
 - Selected - P2P group Owner role established at formation or at an application level
- Provisioning of P2P Group
 - Establishment of P2P group session using appropriate credentials
 - Using Wi-Fi simple configuration to exchange credentials.

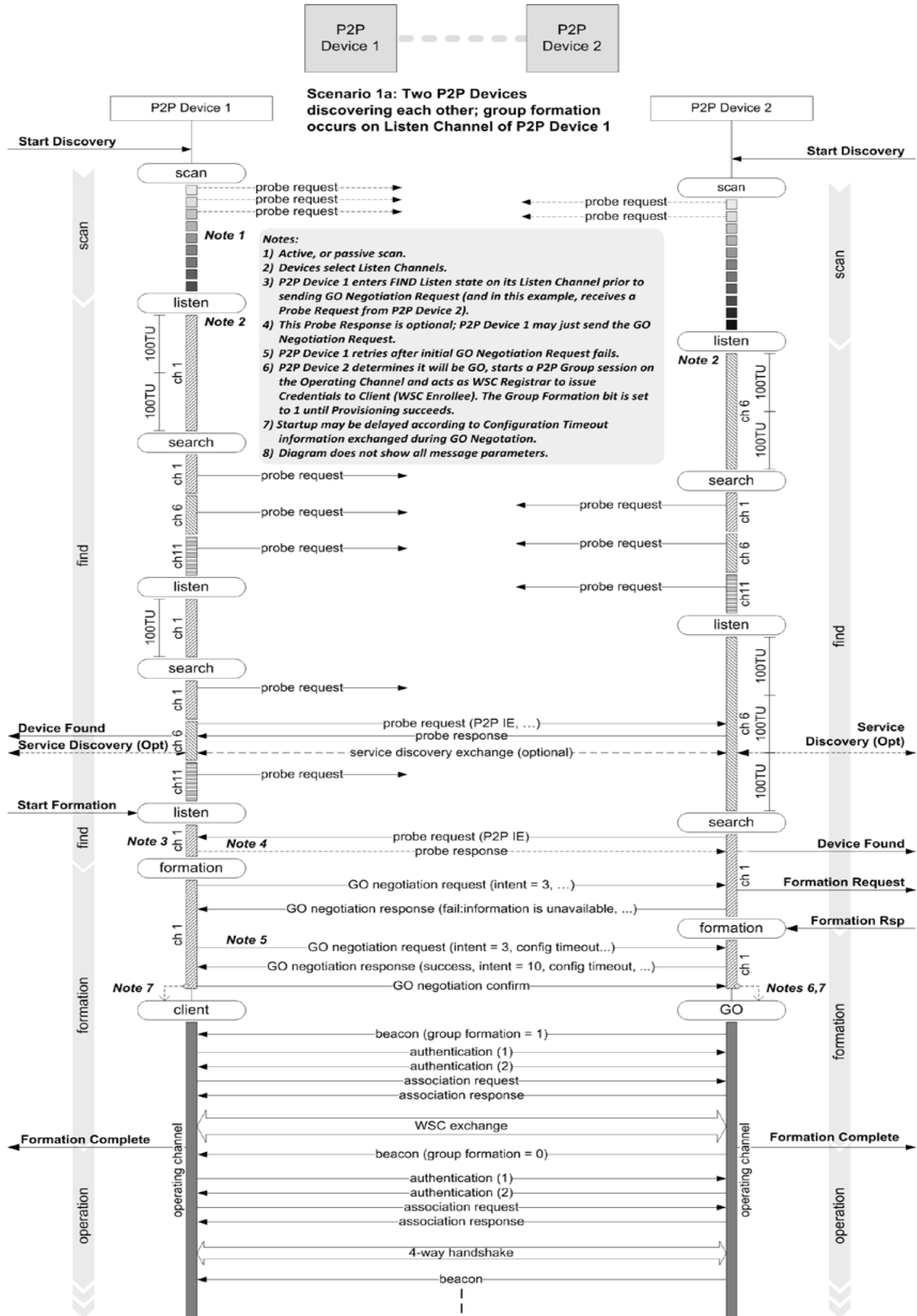
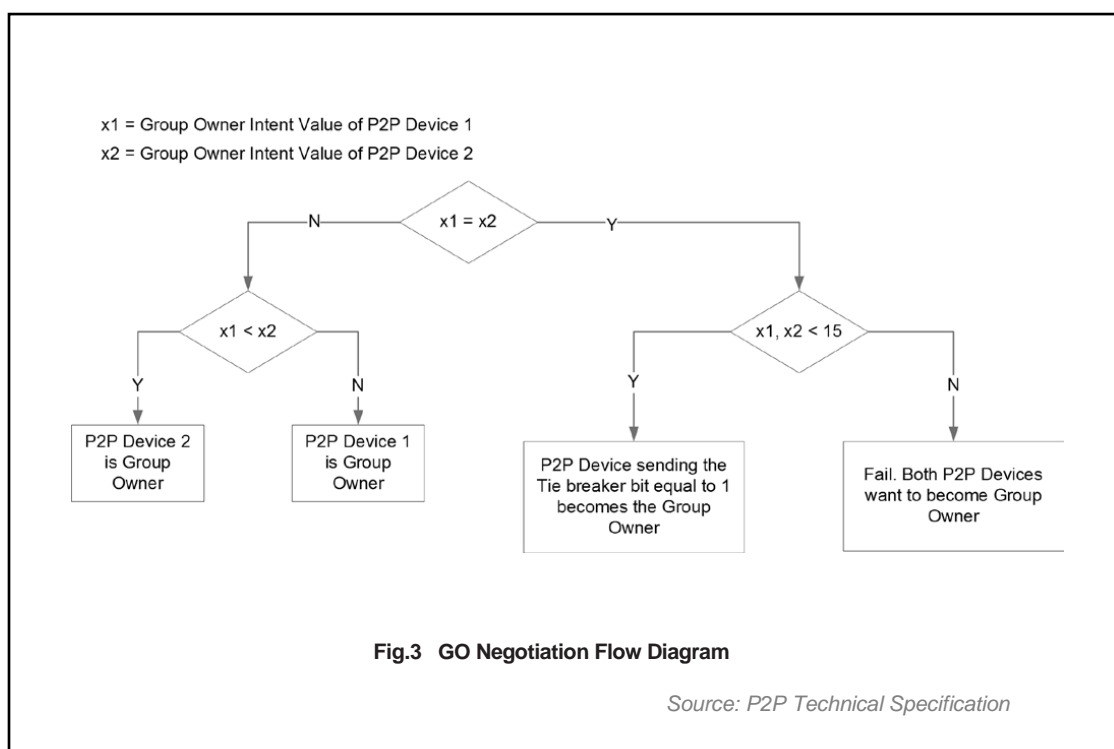


Fig.2. Wi-Fi Direct GO Negotiation and Group Formation Sequence

Source: P2P Technical Specification

i. *Standard*: In this case the P2P devices have first to discover each other, and then negotiate which device will act as P2P GO. Wi-Fi Direct devices usually start by performing traditional Wi-Fi scan (active or passive), by means of which they can discover existent P2P Groups and Wi-Fi networks. After this scan, a new Discovery algorithm is executed. First, a P2P Device selects one of the *Social channels*, namely channels 1, 6 or 11 in the 2.4 GHz band, as its *Listen channel*. Then, it alternates between two states: a search state, in which the device performs active scanning by sending Probe Requests in each of the social channels; and a listen state, in which the device listens for Probe Requests in its listen channel to respond with Probe Responses. Once the two P2P Devices have found each other, they start the GO Negotiation phase. This is implemented using a three-way handshake, namely *GO Negotiation Request/ Response/ Confirmation*, where by the two devices agree on which device will act as P2P GO and on the channel where the group will operate, which can be in the 2.4 GHz or 5GHz bands. In order to agree on the device that will act as P2P GO, P2P devices send a numerical parameter, the *GO Intent value*, within the three-way hand-shake, and the device declaring the highest value becomes the P2P GO. To prevent conflicts when two devices declare the same GO Intent, a *tie-breaker* bit is included in the GO Negotiation Request, which is randomly set every time a GO Negotiation Request is sent.

ii. *Persistent*: During the formation process, P2P devices can declare a group as *persistent*, by using a flag in the P2P Capabilities attribute present in Beacon frames, Probe Responses and GO negotiation frames. In this way, the devices forming the group store network credentials and the assigned P2P GO and Client roles for subsequent re-instantiations of the P2P group. Specifically, after the Discovery phase, if a P2P Device recognizes to have formed a persistent group with the corresponding peer in the past, any of the two P2P devices can use the *Invitation Procedure* (a two-way handshake) to quickly re-instantiate the group. This is shown in Fig 2, where the *Standard* case is assumed as baseline, and the GO Negotiation phase is replaced by the invitation exchange, and the WPS Provisioning phase is significantly reduced because the stored network credentials can be reused.



P2P Invitation procedure: The P2P Invitation Procedure is an optional procedure used for the following:

- A P2P Group Owner invites a P2P Device to become a P2P Client in its P2P Group.

- A P2P Client inviting another P2P Device to join the P2P Group of which the P2P Client is a member.
- Requesting to invoke a Persistent P2P Group for which both P2P Devices have previously been provisioned and one of the Devices is P2P Group Owner for the Persistent P2P Group.

A P2P Device that is invited to join an operational P2P Group through successful completion of the P2P Invitation Procedure, Use Wi-Fi Simple Configuration to obtain Credentials. Provision Discovery and Wi-Fi Simple Configuration will take place on the Operating Channel of the P2P Group Owner.

P2P Invitation Request: A P2P Invitation Request frame may be transmitted by:

1. A P2P Device that is a member of a P2P Group (i.e. P2P Group Owner or P2P Client) to another P2P Device that supports P2P Invitation Procedure and is currently not a member of the P2P Group to invite that P2P Device to join the P2P Group. When used for this purpose, the invitation Type in the Invitation Flags attribute in the P2P Invitation Request frame set to 0.
2. A P2P Device that is a member of a Persistent P2P Group to another member of that P2P Group and one of the Devices is the P2P Group Owner, to request that the P2P Group be invoked. When used for this purpose, the Invitation Type in the Invitation Flags attribute included in the P2P Invitation Request frame shall be set to 1.

P2P Invitation Response: A P2P Invitation Response frame (with the Status attribute set to Success) transmitted by the P2P Group Owner of a Persistent P2P Group in response to a request to invoke that P2P Group, include the P2P Group BSSID, Channel List, Operating Channel and Configuration Timeout attributes to indicate the Group BSSID, potential Operating Channels, intended Operating Channel and any GO Configuration Time.

3.3 Service Discovery

A salient feature of Wi-Fi Direct is the ability to support service discovery at the link layer. In this way, prior to the establishment of a P2P Group, P2P Devices can exchange queries to discover the set of available services and, based on this, decide whether to continue the group formation or not. *Generic Advertisement Protocol* (GAS) specified by 802.11u [5]. GAS is a layer two query /response protocols implemented through the use of public action frames, that allows two non-associated 802.11 devices to exchange queries belonging to a higher layer protocol (e.g. a service discovery protocol). GAS is implemented by means of a generic container that provides fragmentation and reassembly, and allows the recipient device to identify the higher layer protocol being transported. GAS is used as a container for ANQP (Access Network Query Protocol) elements sent between clients and APs.

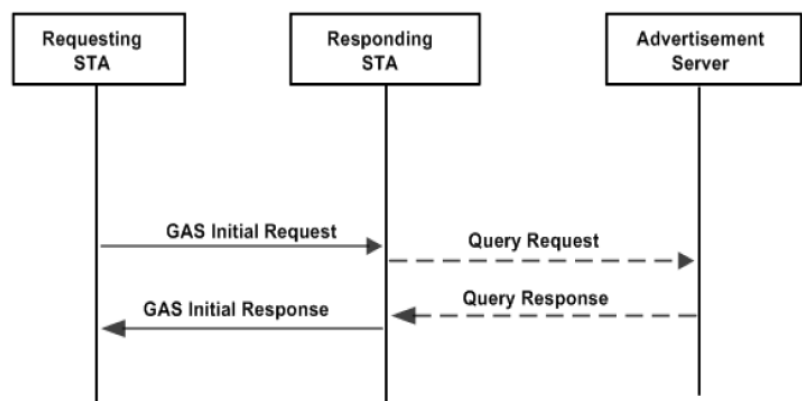
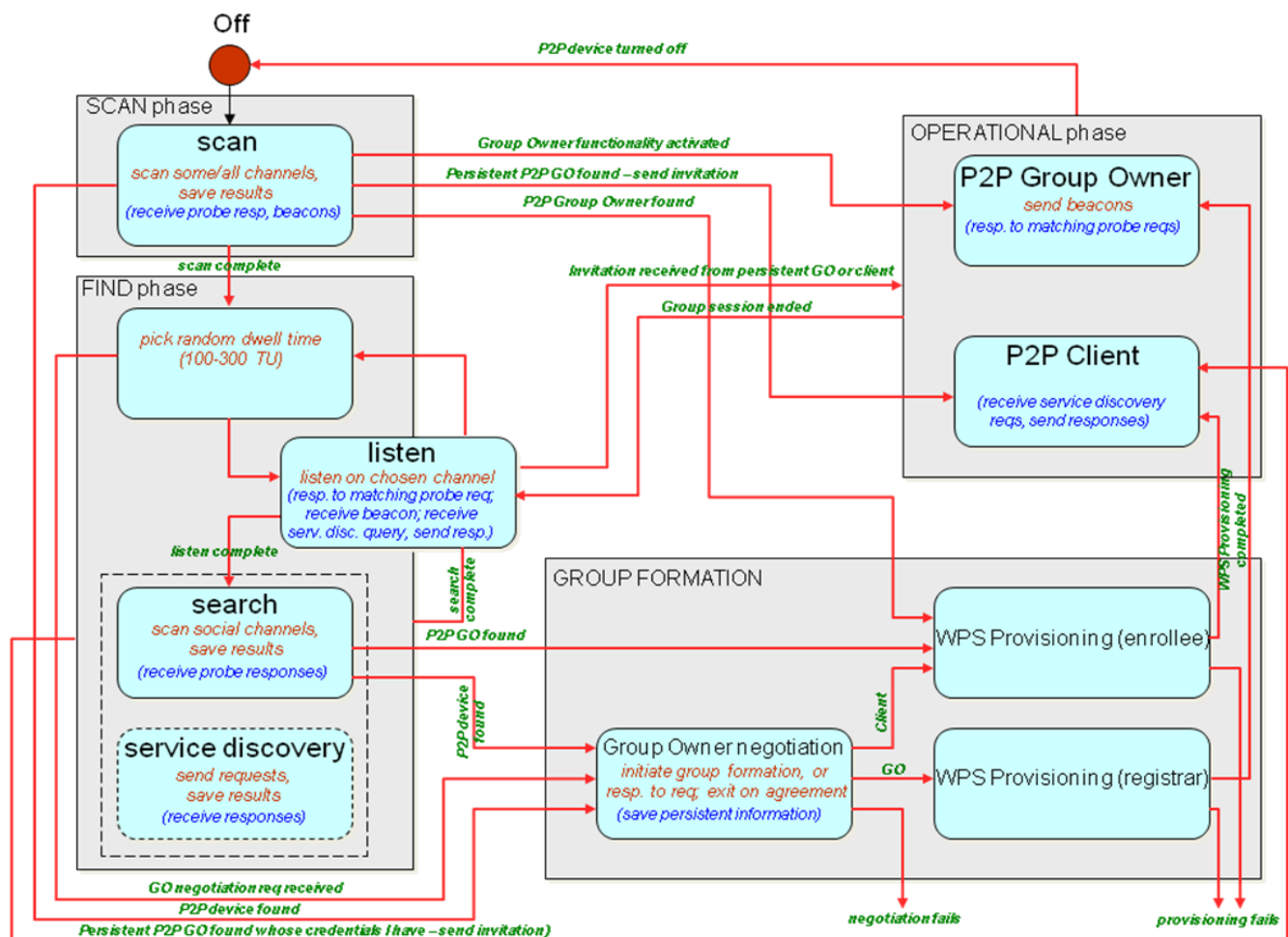


Fig.4. GAS Protocol for ANPQ

Source: P2P Technical Specification

3.4 WFD State Machine



Source: P2P Technical Specification

3.5 Security

Security provisioning starts after discovery has taken place and, if required, the respective roles have been negotiated. Wi-Fi Direct devices are required to implement *Wi-Fi Protected Setup* (WPS) to support a secure connection with minimal user intervention. In particular, WPS allows establishing a secure connection by introducing a PIN in the P2P Client, or pushing a button in the two P2P Devices. Following WPS terminology, the P2P GO is required to implement an internal *Registrar*, and the P2P Client is required to implement an *Enrollee*. The operation of WPS is composed of two parts. In the first part, the internal Registrar is in charge of generating and issuing the network credentials, i.e., security keys, to the Enrollee. WPS is based on WPA-2 security and uses Advanced Encryption Standard (AES)-CCMP as cipher, and a randomly generated Pre-Shared Key (PSK) for mutual authentication. In the second part, the Enrollee (P2P Client) disassociates and reconnects using its new authentication credentials. In this way, if two devices already have the required network credentials (this is the case in the Persistent group

formation), there is no need to trigger the first phase, and they can directly perform the authentication.

3.6 Power Saving

Power saving mechanisms, in current Wi-Fi networks is not defined for APs but only for clients. Wi-Fi Direct defines two new power saving mechanisms: the *Opportunistic Power Save* protocol and the *Notice of Absence* (NoA) protocol. According to rules Of P2P power management, It allow P2P GO to be “absent” for defined periods. A legacy client expects the P2P GO to be always on to prevent use of P2P power saving in a P2P Group which contains a legacy client. The P2P GO is always in the *awake* power state, during the *CTWindow* that is necessary for discoverability & starts at TBTT. *CTWindow* start time and duration is advertised in beacon and probe response frames.

1) *Opportunistic Power Save*: The Opportunistic Power Save protocol (OPS) allows a P2P Group Owner to opportunistically save power when all its associated clients are sleeping. This protocol has a low implementation complexity but, given the fact that the P2P Group Owner can only save power when all its clients are sleeping, the power savings that can be achieved by the P2P Group Owner are limited [6] [OPS are based on the design of the traditional power save mode used by clients in an infrastructure network. A P2PGroup Owner can save power by defining a limited presence period after every Beacon transmission, known as *CTWindow*, where P2P Clients are allowed to transmit. If at the end of the *CTWindow* all associated P2P Clients are sleeping, the P2PGroup Owner is allowed to sleep until the next Beacon time. However, if any P2P Client stays in active mode at the end of the *CTWindow* the P2P Group Owner is forced to remain awake until the next Beacon time.

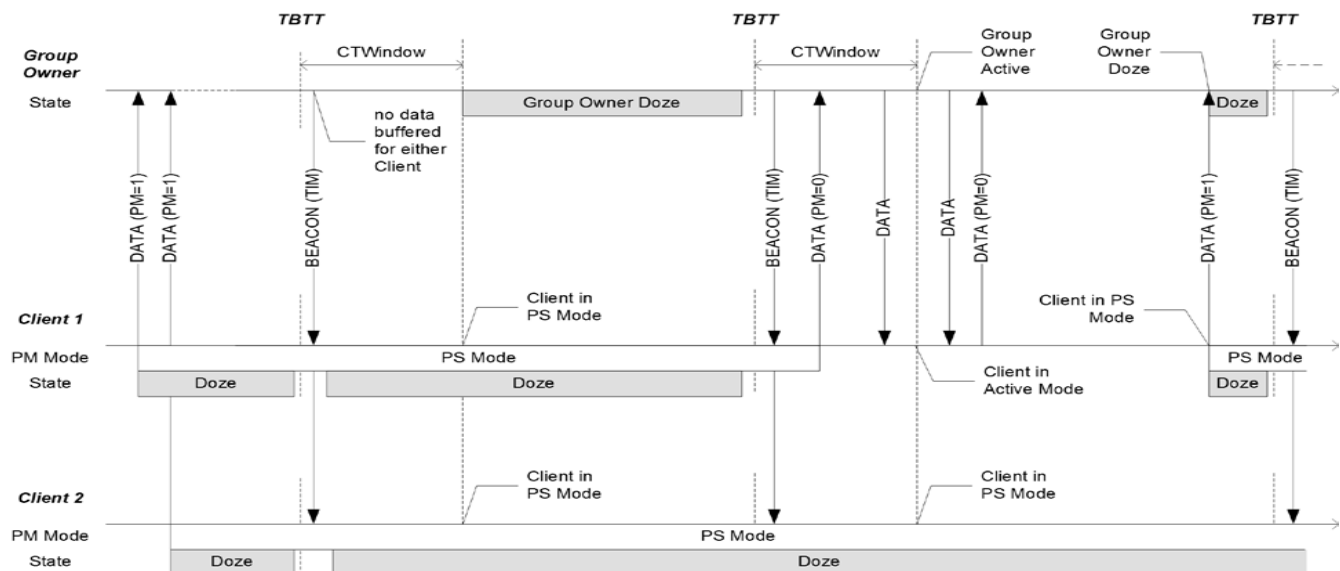


Fig.5. Opportunistic Powersave Operation

Source: P2P Technical Specification

2) *Notice of Absence*: The Notice of Absence (NoA) protocol allows a P2P GO to announce time intervals, referred to as *absence periods*, where P2P Clients are not allowed to access the channel, regardless of whether they are in power save or inactive mode. In this way, a P2P GO can autonomously decide to power down its radio to save energy. Like in the Opportunistic Power Save protocol, in the case of NoA the P2P GO defines absence periods with a signaling element included in Beacon frames and Probe Responses.

In particular, a P2P GO defines a *NoA schedule* using four parameters:

- Duration* that specifies the length of each absence period
- Interval* that specifies the time between consecutive absence periods
- Time* that specifies the start time of the first absence period after the current Beacon frame
- Count* that specifies how many absence periods will be scheduled during the current NoA schedule

A P2P GO can either cancel or update the current NoA schedule at anytime by respectively omitting or modifying the signaling element. P2P Clients always adhere to the most recently received NoA schedule. Fig 6 depicts an example operation of the NoA protocol.

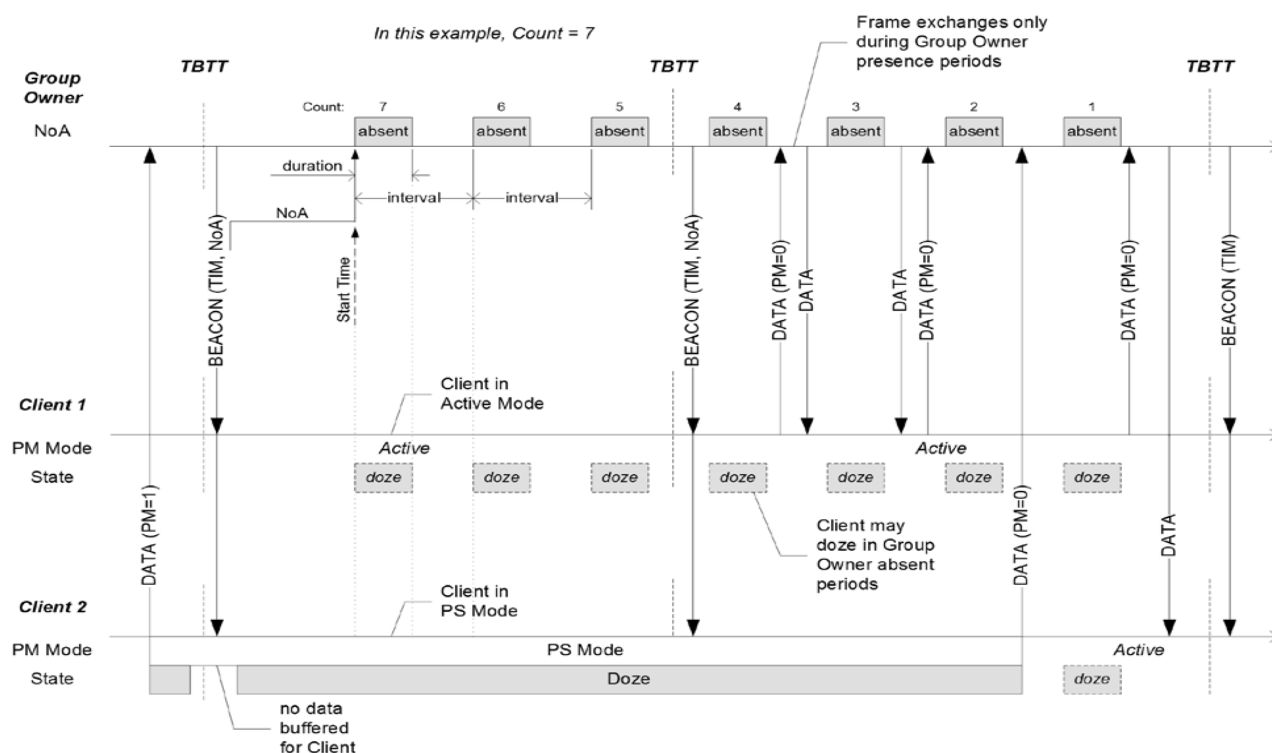


Fig.6. Notice of Absence Powersave Operation

Source: P2P Technical Specification

4.0 PACKET ANALYSIS

This section describes packet details of Wi-Fi Direct protocol.

Wi-Fi Direct IE: The format of the P2P IE is shown in Fig 7. The P2P attributes are defined to have a common general format consisting of a 1 octet P2P Attribute ID field, a 2 octet Length field and variable-length attribute-specific information fields, shown in fig 8.

A P2P Device that encounters an unknown or reserved Attribute ID value in a P2P IE received without error shall ignore that P2P attribute and parse any remaining fields for additional P2P attributes with

Field	Size (Octet)	Value (Hexadecimal)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific usage.
Length	1	variable	Length of the following fields in the IE in octets. The length field is a variable and set to 4 plus the total length of P2P attributes.
OUI	3	50 6F 9A	WFA specific OUI
OUI Type	1	0x09 (to be assigned)	Identifying the type or version of P2P IE. Setting to 0x09 indicates WFA P2P v1.0.
P2P Attributes	Variable		One or more P2P attributes appear in the P2P IE.

Fig.7. P2P IE Format

Source: P2P Technical Specification

recognizable Attribute ID values. A P2P Device that encounters a recognizable but unexpected Attribute ID value in the received P2P IE may ignore that P2P attribute. More than one P2P IE may be included in a single frame. If multiple P2P IEs are present, the complete P2P attribute data consists of the concatenation of the P2P Attribute fields of the P2P IEs. The P2P Attributes field of each P2P IE may be any length up to the maximum (251 octets).

Field	Size (Octet)	Value (Hexadecimal)	Description
Attribute ID	1	variable	Identifying the type or version of P2P attribute.
Length	2	variable	Length of the following fields in the attribute.
Attribute body field	Variable		Attribute specific information fields.

Fig.8. General Format of P2P attributes

Source: P2P Technical Specification

The P2P Capability attribute contains a set of parameters that can be used to establish a P2P connection. The format of the P2P Capability attribute is shown Fig 9.

Field	Size (Octet)	Value	Description
Attribute ID	1	2	Identifying the type of P2P attribute.
Length	2	2	Length of the following fields in the attribute.
Device Compatibility Bitmap	1	variable	A set of parameters indicating P2P Device's capabilities.
Group Compatibility Bitmap	1	variable	A set of parameters indicating the current state of a P2P Group.

Fig.9. P2P Capability attribute format

Source: P2P Technical Specification

The Public Action frame format (as defined in IEEE 802.11k) is used to define the P2P public action frames. The general format of the P2P public action frames is shown in Fig 10.

Field	Size (Octet)	Value (Hexadecimal)	Description
Category	1	0x04	IEEE 802.11 public action usage
Action field	1	0x09	IEEE 802.11 vendor specific usage
OUI	3	50 6F 9A	WFA specific OUI
OUI Type	1	0x09 (to be assigned)	Identifying the type of version of action frame. Setting to 09 indicates WFA P2P v1.0
OUI Subtype	1		Identifying the type of P2P public action frame.
Dialogue Token	1		Set to non zero value to identify the request/ response transaction.
Elements	variable		Including P2P IE or any other information elements defined in IEEE std. 802.11-2007

Fig.10. General Format of P2P Public Action Frame

Source: P2P Technical Specification

The Wi-Fi Direct sniffer capture is shown below. Various tools are available to capture the air packets like wireshark and omnipeek. The format of the P2P Information Element is shown Fig 11 and Fig 12.

Wi-Fi Direct	
Element ID:	221 Vendor Specific - Wi-Fi Alliance [163]
Length:	39 [164]
OUI:	50-6F-9A Wi-Fi Alliance [165-167]
OUI Type:	0x09 Wi-Fi Direct [168]
P2P Attribute	
ID:	2 P2P Capability [169]
Length:	2 [170-171]
Device Capability:	%00100011 [172]
	xx... .. Reserved
	..1. Processes Invitation Procedure
	...0 Device Limit not set
 0... Infrastructure Managed not set
0.. Concurrent Operation not supported
1. P2P Client Discovery supported
1 Service Discovery supported
Group Capability:	
	%00000000 [173]
	x... Reserved
	.0.. Group Formation - Not Owner
	..0. Persistent Reconnect not supported
	...0 Cross Connection not supported
 0... Intra-BSS Distribution not supported
0.. P2P Group Limit not set
0. Persistent P2P Group not set
0 P2P Group Owner not set
P2P Attribute	
ID:	13 P2P Device Info [174]
Length:	27 [175-176]
Device Address:	00:80:E1:28:79:AC Stmicroele:28:79:AC [177-182]
Config Methods:	0x0188 [183-184]
	xxxx xxx. Reserved
1 Keypad: yes
 1... Pushbutton: yes
0.. NFC Interface: no
0. Integrated NFC Token: no
0 External NFC Token: no
 1... Display: yes
0.. Label: no
0. Ethernet: no
0 USB (Flash Drive): no

Fig.11. P2P Information Element shown from a captured Packet












































	802.11 Management - Action	
	Category Code:	4 <i>Public Action</i> [24]
	Action Code:	9 <i>Vendor Specific</i> [25]
	OUI:	50-6F-9A <i>Wi-Fi Alliance</i> [26-28]
	Subtype:	9 [29]
	OUI Subtype:	0 <i>GO Negotiation Request</i> [30]
	Dialog Token:	150 [31]
	Wi-Fi Direct	
	Element ID:	221 <i>Vendor Specific - Wi-Fi Alliance</i> [32]
	Length:	92 [33]
	OUI:	50-6F-9A <i>Wi-Fi Alliance</i> [34-36]
	OUI Type:	0x09 <i>Wi-Fi Direct</i> [37]
	P2P Attribute	
	ID:	2 <i>P2P Capability</i> [38]
	Length:	2 [39-40]
	Device Capability:	%00100011 [41]
		xx.. <i>Reserved</i>
		..1. <i>Processes Invitation Procedure</i>
		...0 <i>Device Limit not set</i>
	 0... <i>Infrastructure Managed not set</i>
	0.. <i>Concurrent Operation not supported</i>
	1. <i>P2P Client Discovery supported</i>
	1 <i>Service Discovery supported</i>
	Group Capability:	%00001000 [42]
		x... <i>Reserved</i>
		.0.. <i>Group Formation - Not Owner</i>
		..0. <i>Persistent Reconnect not supported</i>
		...0 <i>Cross Connection not supported</i>
	 1... <i>Intra-BSS Distribution supported</i>
	0.. <i>P2P Group Limit not set</i>
	0. <i>Persistent P2P Group not set</i>
	0 <i>P2P Group Owner not set</i>
	P2P Attribute	
	ID:	4 <i>Group Owner Intent</i> [43]
	Length:	1 [44-45]
	GO Intent	
	Intent:	15 [46 Mask 0xFE]
	Tie Breaker:	0 [46 Mask 0x01]
	P2P Attribute	
	ID:	5 <i>Configuration Timeout</i> [47]
	Length:	2 [48-49]
	GO Config Timeout:	100 <i>(1000 msec)</i> [50]
	Client Config Timeout:	20 <i>(200 msec)</i> [51]

Fig.12. P2P Packet Captured with detail view as shown in Omnipeek

5.0 TESTING TECHNIQUES

Testing for P2P devices involves testing of both P2P client and P2P GO. For testing of P2P client DUT is either not associated to a P2P Group Owner (GO) or if the device is already a P2P Client in a Group it uses its P2P Device Address to communicate with another P2P device.

For P2P GO testing, the device under test is acting as a P2P Group Owner of a Group. In this mode the device may have none, one or more P2P Clients or legacy STAs attached.

The WFA Sigma Automation Suite is used for the WFD Certification. This tool suite provides configuration, test control, traffic generation, and results analysis services.

Sigma Testbed Setup

P2P Device can be tested for conformance, stability and performance. Tools like Ixia Chariot are used to analyzing and measure the throughput of devices.

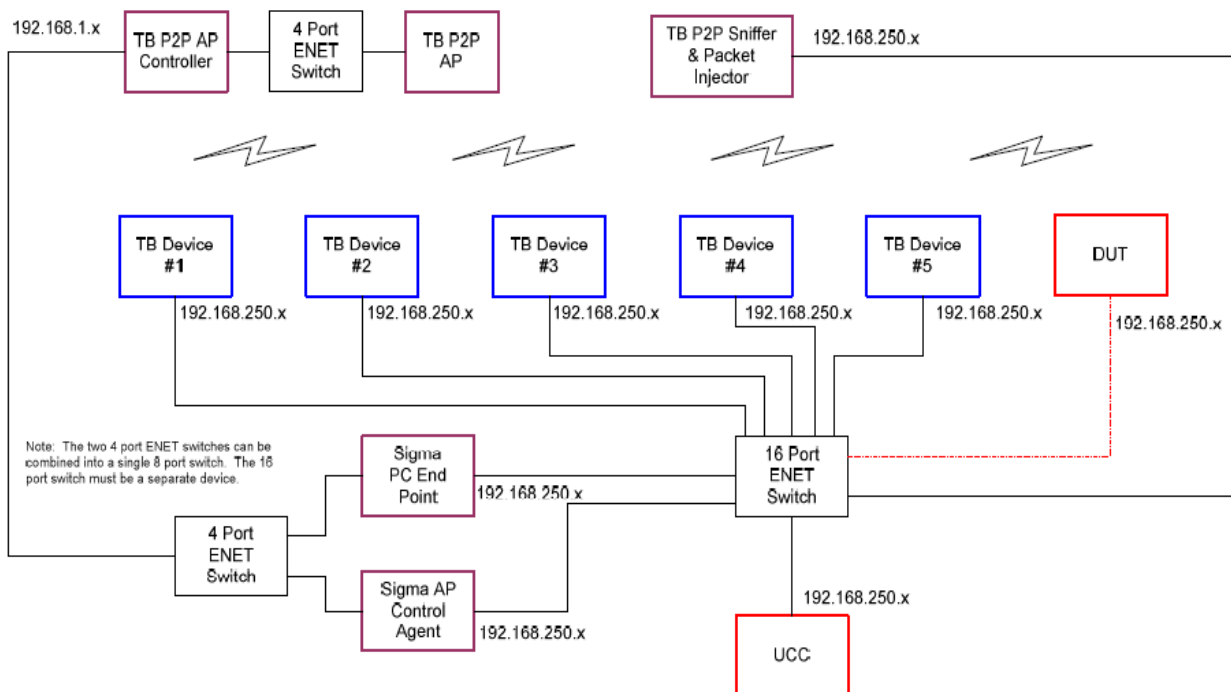


Fig.13. P2P Certification Test Configuration System

6.0 REFERENCES

- [1] IEEE 802.11-2007 Standard, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2007.
- [2] J.R. Jiang, Y.C. Tseng C.S. Hsu and T.H. Lai.(2005)Quorum-based asynchronous power-saving protocols for 802.11 ad hoc networks.
- [3] Wi-Fi Alliance, P2P Technical Group, *Wi-Fi Peer-to-Peer (P2P) Technical Specification v1.0*, December 2009.
- [4] *Wi-Fi Alliance, Wi-Fi Protected Setup Specification v1.0h*, Dec. 2006.
- [5] 802.11u-2011 - *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 9: Interworking with External Networks*.
- [6] OPSPM - *Opportunistic Power Save Mode for Infrastructure IEEE 802.11 WLAN*;
<http://www.ece.iisc.ernet.in/~anurag/papers/anurag/agarwal-et-al10opsm-wlans.pdf>
- [7] Wi-Fi Direct in Linux, <http://linuxwireless.org/en/developers/p2p/>
- [8] Wi-Fi Alliance, Quality of Service (QoS) Task Group, *Wi-i Multi- media (including WMM PowerSave) Specification v1.1*, 2005.
- [9] IEEE 802.11z-2010 - *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Extensions to Direct-Link Setup (DLS)*.

PROPRIETARY NOTICE

All rights reserved. This publication and its contents are proprietary to Hughes Systique Corporation. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Systique Corporation, 15245 Shady Grove Road, Suite 330, Rockville, MD 20850.

Copyright © 2006 Hughes Systique Corporation

CONTACT INFORMATION:

phone: +1.301.527.1629

fax: +1.301.527.1690

email: whitepaper@hsc.com

web: www.hsc.com

APPENDIX A ABOUT HUGHES SYSTIQUE CORPORATION

HUGHES Systique Corporation (HSC), part of the HUGHES group of companies, is a leading Consulting and Software company focused on Communications and Automotive Telematics. HSC is headquartered in Rockville, Maryland USA with its development centre in Gurgaon, India.

SERVICES OFFERED:

Technology Consulting & Architecture: Leverage extensive knowledge and experience of our domain experts to define product requirements, validate technology plans, and provide network level consulting services and deployment of several successful products from conceptualization to market delivery.

Development & Maintenance Services: We can help you design, develop and maintain software for diverse areas in the communication industry. We have a well-defined software development process, comprising of complete SDLC from requirement analysis to the deployment and post production support.

Testing : We have extensive experience in testing methodologies and processes and offer Performance testing (with bench marking metrics), Protocol testing, Conformance testing, Stress testing, White-box and black-box testing, Regression testing and Interoperability testing to our clients

System Integration : As system integrators of choice HSC works with global names to architect, integrate, deploy and manage their suite of OSS, BSS, VAS and IN in wireless (VoIP & IMS), wireline and hybrid networks.: NMS, Service Management & Provisioning .

DOMAIN EXPERTISE:

Terminals

- Terminal Platforms : iPhone, Android, Symbian, Windows CE/Mobile, BREW, PalmOS
- Middleware Experience & Applications : J2ME , IMS Client & OMA PoC,

Access

- Wired Access : PON & DSL, IP-DSLAM,
- Wireless Access : WLAN/WiMAX / LTE, UMTS, 2.5G, 2G ,Satellite Communication

Core Network

- IMS/3GPP , IPTV , SBC, Interworking , Switching solutions, VoIP

Applications

- Technologies : C, Java/J2ME, C++, Flash/lite,SIP, Presence, Location, AJAX/Mash
- Middleware: GlassFish, BEA, JBOSS, WebSphere, Tomcat, Apache etc.

Management & Back Office:

- Billing & OSS , Knowledge of COTS products , Mediation, CRM
- Network Management : NM Protocols, Java technologies,, Knowledge of COTS NM products, FCAPS, Security & Authentication

Platforms

- Embedded: Design, Development and Porting - RTOS, Device Drivers, Communications / Switching devices, Infrastructure components. Usage and Understanding of Debugging tools.
- FPGA & DSP : Design, System Prototyping. Re-engineering, System Verification, Testing

Automotive Telematics

- In Car unit (ECU) software design with CAN B & CAN C
- Telematics Network Design (CDMA, GSM, GPRS/UMTS)

BENEFITS:

- **Reduced Time to market :** Complement your existing skills, Experience in development-to-deployment in complex communication systems, with key resources available at all times

- **Stretch your R&D dollars** : Best Shore” strategy to outsourcing, World class processes, Insulate from resource fluctuations

CONTACT INFORMATION:

phone: +1.301.527.1629

fax: +1.301.527.1690

email: whitepaper@hsc.com

web: www.hsc.com