Wi-Fi CERTIFIED Wi-Fi Direct™

Personal, portable Wi-Fi® technology

Wi-Fi Alliance®
October 2010

Executive Summary

Wi-Fi CERTIFIED Wi-Fi Direct™ devices can connect in a way that makes it more simple and convenient than ever for users to print, share, sync and display. Wi-Fi Direct devices can connect directly to one another without access to a traditional network, so mobile phones, cameras, printers, PCs, and gaming devices can connect to each other directly to transfer content and share applications anytime and anywhere. Devices can make a one-to-one connection, or a group of several devices can connect simultaneously. They can connect for a single exchange, or they can retain the memory of the connection and link together each time they are in proximity.

Around the globe, people are creating, storing, accessing and sharing more songs, videos, pictures and documents than ever before. Millennials in the US, people between the ages of 18-29, have on average 2400 songs, videos and pictures stored on digital devices. That growing number is echoed by their peers in China, Japan and Korea.[1] They are used to gathering around a single digital camera to look at pictures with friends and family, or around a single handheld or laptop screen to watch videos. Now Wi-Fi Direct products allow them to connect

Digital Content Stored Worldwide
Wakefield Research - August 2010
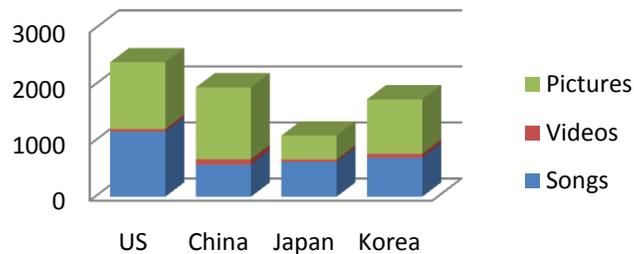
Figure 1: US Millennials store an average of 2400 songs, photos and videos on digital devices

directly with each others' devices to share those pictures, games and video, or display them on a nearby monitor or TV for easy viewing.

The introduction of the Wi-Fi Alliance Peer-to-Peer Specification and certification testing program dramatically expands peer-to-peer connectivity for consumers by introducing an interoperable technology with distinctive new features. In a recent study, US consumers revealed that they would most want to use direct connections for instant messaging, sharing pictures with friends and family, displaying those pictures from a portable device to a monitor or TV screen, video chatting, and playing video games with others while not at home, such as when using public transit.[2] Consumers in China, Japan, and Korea said the same.

This white paper is describes Wi-Fi Peer-to-Peer technology (P2P). Wi-Fi CERTIFIED™ devices implementing this technology will bear the certification mark Wi-Fi CERTIFIED Wi-Fi Direct™. A technical description of the technology can be found in the Wi-Fi Alliance Peer-to-Peer Specification.

---

[1] Wakefield Research, Global Wi-Fi Survey, August 2010.
[2] Wakefield Research, Global Wi-Fi Survey, August 2010.

Contents

Note on Terminology: The Wi-Fi Alliance Peer-to-Peer Specification defines a new peer-to-peer capability for Wi-Fi devices. The Wi-Fi Direct trademark identifies devices that have successfully completed interoperability certification testing for the features defined in the Wi-Fi Alliance Peer-to-Peer Specification. In this document, the terms Peer-to-Peer, P2P, and Wi-Fi P2P are used interchangeably to refer to the underlying technology developed in Wi-Fi Alliance; Wi-Fi Direct is only used to refer to the certification mark or products which have achieved the certification.

Wi-Fi Technology Evolves

As Wi-Fi begins its second decade, the members of the Wi-Fi Alliance have developed a specification to expand how consumers can use Wi-Fi. Wi-Fi Direct-certified devices have a new capability that allows the creation of direct connections between Wi-Fi client devices without requiring the presence of a traditional Wi-Fi infrastructure network (i.e., AP or router). Devices certified to the Wi-Fi Alliance Peer-to-Peer Specification will be able to bear the Wi-Fi CERTIFIED Wi-Fi Direct certification mark.
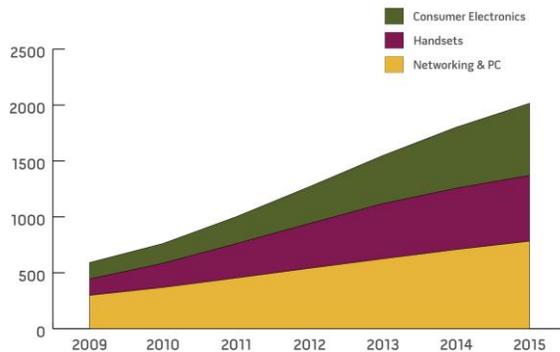

Figure 2: Wi-Fi shipments continue to grow each year, with more than 1 billion devices in use today.

Today, roughly 10% of all people in the world use Wi-Fi to stay connected.[3] There are more than 1 billion Wi-Fi devices in use today, with an estimated 580 million units shipped in 2009. Shipments for 2011 are forecasted at 1 billion devices, growing to 1.5 billion by 2013 (see Figure 2).[4] Wi-Fi is widely available in homes, Wi-Fi hotspots, enterprise environments, and is found in many types of devices, including notebook computers, cameras, media players, photo frames, TVs, gaming devices, and mobile phones, among others. At the time of this paper's publication, the Wi-Fi Alliance has more than 350 member companies and has completed more than 8,000 product certifications since March 2000.

The introduction of Wi-Fi CERTIFIED Wi-Fi Direct devices extends Wi-Fi's utility at the center of a seamless connectivity experience. The technology greatly enhances the portability of content and applications across all of a user's devices with a single industry-wide technology, allowing users to access movies, music, and photos on-the-go. Equipment vendors and content providers also benefit, as multiple applications – including IP-based connectivity, legacy interoperability, and others – can be transparently interconnected wherever you go.

Wi-Fi Direct-certified devices support connection with existing legacy Wi-Fi devices. In this way, a direct connection capability is possible on the hundreds of millions of legacy Wi-Fi CERTIFIED devices (802.11 a/g/n) already deployed.

Wi-Fi Peer-to-Peer technology builds on traditional Wi-Fi strengths like performance, security, ease of use and ubiquity, and adds features that optimize it for consumer uses that don't require access to an infrastructure network. Rather than connecting first to an infrastructure network and then connecting to another networked device, users can connect directly to those devices offering the services they need. This allows, for example, a user to show friends the photos on his mobile phone by connecting directly to a television and displaying the images, regardless of whether an infrastructure network is available to both devices.

---

[3] Wi-Fi Alliance estimate of installed base of Wi-Fi devices, 2009.
[4] ABI Research, 2010.

Wi-Fi Direct

Many consumers associate Wi-Fi with Internet connectivity. Devices certified for Wi-Fi Direct extend the technology's reach to include the simple, direct connections that many users may accomplish using cables today. Some of the benefits consumers will see from Wi-Fi Direct devices include:

- **Mobility & Portability:** Wi-Fi Direct devices can connect anytime, anywhere connections. Since a Wi-Fi router or AP is not required, Wi-Fi devices can be connected everywhere.
- **Immediate Utility:** Users will have the ability to create direct connections with the very first Wi-Fi Direct certified devices they bring home. For example, a new Wi-Fi Direct laptop can create direct connections with a user's existing legacy Wi-Fi devices.
- **Ease of Use:** Wi-Fi Direct Device Discovery and Service Discovery features allow users to identify available devices and services before establishing a connection. For example, if a user would like to print, they can learn which Wi-Fi networks have a printer.
- **Simple Secure Connections:** Wi-Fi Direct devices use Wi-Fi Protected Setup™ to make it simple to create secure connections between devices. Users either press a button on both devices or type in a PIN (i.e., displayed by a device) to easily create a secure connection.

P2P technology plays a role anywhere a quick connection is desired. Here are some examples of how Wi-Fi Direct devices expand redefines the connected experience for consumers:

- Nora needs to print her term paper before heading to class. Her laptop has permission to access the university's network, but she is not allowed to connect her printer to the network. In her dorm room using her Wi-Fi Direct laptop, she prints directly to her Wi-Fi printer while continuing to check email over the university Wi-Fi network.
- Bert and Fergus invite the guests at their party to use the cameras on their mobile phones to capture the party, and directly share images with each other.
- Joe is commuting to work on the train after a once-in-a-lifetime vacation overseas. He makes use of the time to transfer his photos directly from his Wi-Fi-enabled camera to his tablet and culls through them to find the best ones. After work, he visits friends and displays the photos on their Wi-Fi-enabled television. .
- Kevin has been travelling for two weeks using his netbook. When he returns to the office, he syncs the new files he has created on his netbook with his desktop PC.
- Kyle's friends Taylor, Jett and Ava come to his house after school to play video games. The group bypasses the home network and directly connects their handheld gaming devices to engage in mortal combat. Jett prevails. Later that evening, Kyle connects to his home network and challenges Jett to a rematch over the Internet.

In managed environments such as enterprise or hotspot networks, P2P provides simple, convenient connectivity while augmenting the strong security of an infrastructure network. For example, guest devices requiring access to a printer are typically given permission to join the LAN or WLAN. This requires additional configuration complexity and potentially exposes network resources. A Wi-Fi Direct guest device can connect directly to a printer without having to be given access to any other network resource. All Wi-Fi Direct devices make their presence and settings known so they can be integrated into management systems e.g. rogue AP detection. Optional managed device capabilities allow IT managers to further optimize and define the behaviors of Wi-Fi Direct devices.

A Platform for Innovation

Wi-Fi Peer-to-Peer technology has been designed to be implemented on the same silicon as the majority of new devices that support Wi-Fi. As a result, the new capabilities will not require a significant increase in software or CPU capability.

Wi-Fi Peer-to-Peer empowers developers to offer users anytime, anywhere connectivity and adds additional capabilities to address the needs of fully portable connections. For many applications developers, there will be little, if any, difference in the development process. In addition, the IP links make it straightforward for enabled devices to leverage the constantly rising and evolving wave of new networked applications.

Developers have the option of keeping the connection process separate from the application or integrating the connection within the application. For example, consider a user who wants to display a photo. With Service Discovery, the application can offer to connect to only those devices which have a large display (e.g., a picture frame, TV or laptop) or printer. If only one device is available, application developers have the option of automatically selecting it for the user. Once a persistent connection is made, it can be used again in the future without any further configuration.

Having a connection framework that is distinct from applications makes for efficient processing and offers developers a flexible way to implement designs. The P2P connection can be managed by the application, a management function, or even the operating system. In addition, this flexible approach avoids forcing the link to be dedicated to a single task and locking out the link from being used by other applications.

P2P builds on Wi-Fi's traditional strengths…

- Throughput and range of traditional Wi-Fi technology (up to Wi-Fi CERTIFIED 802.11n)
- Compatibility with legacy Wi-Fi CERTIFIED devices
- Support for 2.4 and 5 GHz operation
- Flexible IP connection
- Best in class security: WPA2
- Simple configuration: Wi-Fi Protected Setup

… and introduces important new capabilities.

- Automatic device discovery
- Pre-connection service discovery
- Enhanced power management modes
- Support for multiple simultaneous connections (concurrent connections)
- Separate security domains for infrastructure and direct connections
- Enterprise-friendly device management
- Internet connection sharing

Technology Basics

By definition, a Wi-Fi CERTIFIED Wi-Fi Direct device is capable of a peer-to-peer connection, and can support either an infrastructure or a P2P connection. Wi-Fi Direct devices have the ability to join infrastructure networks as typical stations (STAs), and must support Wi-Fi Protected Setup enrollee functionality.

Wi-Fi Direct devices connect by forming Groups (in a one-to-one or one-to-many topology) that function in a manner similar to an infrastructure BSS. A single Wi-Fi Direct device is in charge of the Group, including controlling which devices are allowed to join and when the Group is started

and terminated. This device will appear as an AP to legacy Clients. , and provides some of the services commonly provided by an infrastructure AP. Examples include:

BSS functionality, Wi-Fi Protected Setup Internal Registrar functionality and communication between Clients in the Group. Optional features such as simultaneous (concurrent) connection with an infrastructure network and sharing of that infrastructure connection may also be provided.
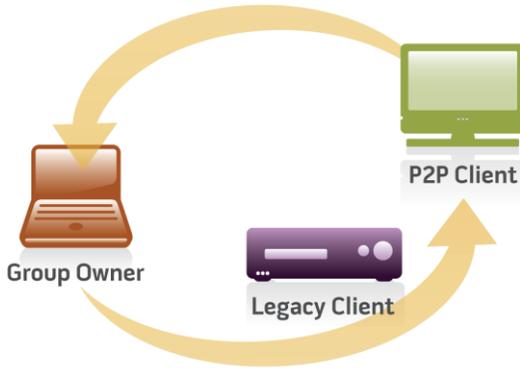

Figure 3: Group with Wi-Fi Direct Client, and legacy device.

Note that because Wi-Fi Direct devices do not duplicate the full functionality of infrastructure APs, traditional APs will continue to be the best choice for meeting the needs of stationary, multipurpose networks in homes, hotspots and enterprises.

All Wi-Fi Direct devices must be capable of being in charge of a Group, and must be able to negotiate which device adopts this role when forming a Group with another Wi-Fi Direct device. Wi-Fi Direct devices must also support mandatory Discovery and Power Management mechanisms. Wi-Fi Direct devices may support optional features including Managed Device mechanisms and Concurrent infrastructure connections.

A Group may be comprised of both Wi-Fi Direct devices and legacy devices (i.e., Wi-Fi CERTIFIED devices that are not compliant with the Wi-Fi Alliance Peer-to-Peer Specification). Legacy Devices can only function as Clients within a Group.

Key Mechanisms

Table 1 lists the key mechanisms defined in the Wi-Fi Alliance Peer-to-Peer Specification.

Table 1: Key Mechanisms	Mandatory	Optional
Device Discovery Mechanism to find Wi-Fi Direct devices and exchange device information.	X	
Service Discovery Mechanism to facilitate discovery of higher-layer services. Can be exercised prior to establishing a Wi-Fi Direct device connection.		X
Group Formation Mechanism to determine which Wi-Fi Direct device is in charge of the Group.	X	
Invitation A mechanism that allows a Wi-Fi Direct device to invite another Wi-Fi Direct device to join an existing Group.		X
Client Discovery Mechanism enabling a Wi-Fi Direct device to discover which Wi-Fi Direct devices are in an existing Group.	X	

Power Management		
P2P-PS and P2P-WMM®-PS Adaptations of legacy Power Save and WMM-Power Save mechanisms that enable additional savings for Wi-Fi Direct devices.	X	
Notice of Absence New technique enabling a Wi-Fi Direct device that is in charge of a Group to reduce power consumption by communicating a planned absence.	X	
Opportunistic Power Save New technique enabling Wi-Fi Direct device that is in charge of a group to reduce power consumption by entering a doze state while connected Wi-Fi Direct devices are dozing.	X	

Device Discovery

Device Discovery is used to identify other Wi-Fi Direct devices and establish a connection. It is accomplished using a scan similar to that used to discover infrastructure APs. Users can select a discovered device for connection. If the target is not already part of a Group, a new Group is formed. If the target is already part of a Group, the searching Wi-Fi Direct device may attempt to join the existing Group. Wi-Fi Protected Setup is used to obtain credentials and authenticate the searching Wi-Fi Direct device.

Service Discovery

Service Discovery is an optional feature that enables the advertisement of services supported by higher layer applications (i.e., Bonjour, UPnP, Web Service Discovery) to other Wi-Fi Direct devices. Service Discovery can be performed at any time (e.g. even before a connection is formed) with any other discovered Wi-Fi Direct device.

For example, if a user wants to print a photo, the printing application can identify which Wi-Fi Direct devices can provide printing services and present a compatible list of options to the user. This can prevent frustration that may arise by attempting to connect to an incompatible printer. Implementation of Service Discovery is vendor-specific.
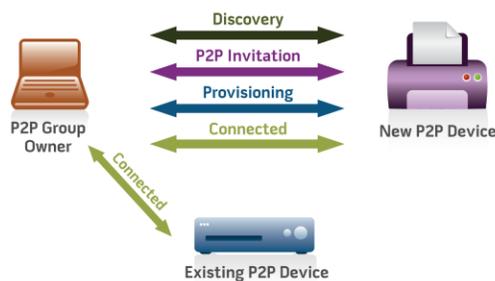

Figure 4: Adding a Device by Invitation. The P2P Invitational Procedure enables a Wi-Fi Direct device to become a P2P Client of an existing P2P Group.

Creating a Group

A Group may be created by a single Wi-Fi Direct device. This is required when connecting a legacy device and may be desirable when creating a Group to offer a specific service e.g. Internet connection sharing. When forming a connection between two Wi-Fi Direct devices a Group may be formed automatically; in this case the devices will negotiate to determine which device is in charge of the Group. The device in charge of the Group always decides if this is a temporary (single instance) or persistent (multiple, recurring use) Group.

After a Group is formed, a Wi-Fi Direct device may invite another Wi-Fi Direct device to join the Group (see Figure 4). The optional Invitation mechanism can also be used to request that a previously used persistent Group be reformed. The decision of whether or not to accept an invitation is left to the invited Wi-Fi Direct device.

The Client Discovery capability makes it easier for users to locate and connect to a specific device or device type. For example, a camera can query to see if any Wi-Fi Direct devices are printers.

Power Management

Efficient use of power is critical for portable devices. The P2P Specification includes power management mechanisms that can reduce power consumption for devices regardless of role within a Group, while maintaining valuable discovery capabilities. While all Wi-Fi Direct devices implement these mechanisms, realization of power savings will depend on the settings and interaction between the devices in a given environment.

Some of the Power Management capabilities are based on standard Wi-Fi Power Save and WMM-Power Save, with adapted mechanisms referred to as P2P-PS and P2P-WMM-Power Save. The P2P Specification introduces two new power savings mechanisms to enable a device in charge of a Group to save power: Opportunistic Power Save and Notice of Absence. These mechanisms may be used together to maximize doze time - a particularly important capability since in many cases Wi-Fi Direct devices are battery-operated.

The Notice of Absence mechanism makes it possible to signal a planned absence – either single or periodic. Opportunistic Power Save allows to the Wi-Fi Direct device in charge of the Group to save power by entering a doze state when all connected Wi-Fi Direct devices are also in a doze state. To maintain Device Discoverability while using Power Management, the Wi-Fi Direct device in charge of the Group is available on a periodic basis. Searching devices are aware that Power Save mechanisms may be in use. Power management mechanisms are available only for use in Groups in which only Wi-Fi Direct devices are associated. If legacy devices are present, these power management functions cannot be employed.

Important Capabilities

Table 2 lists important capabilities introduced in the Wi-Fi Alliance Peer-to-Peer Specification.

Table 2: Important Capabilities	Mandatory	Optional
Persistent Groups A mechanism that allows a previously established Group to be re-invoked at a future time without re-provisioning.		X
Concurrent Connection Capability of a Wi-Fi Direct Device to maintain multiple connections simultaneously. Connections can be to Groups and/or traditional WLAN.		X
Multiple Groups Wi-Fi Direct Device maintains membership in multiple Groups simultaneously.		X
Cross-connection Allows Wi-Fi Direct device in charge of a Group to provide infrastructure access to other devices in the Group.		X

Managed Device Mechanism allowing a Wi-Fi Direct device to respond to management direction from an AP regarding coexistence, channel selection, or power limitations.		X

Persistent Groups

Groups may be re-invoked for additional sessions after initial formation. For example, a laptop could create a Persistent Group that comprised of the laptop and a printer that is restarted each time a print request is made if the printer is discovered. Persistent Groups may be restarted without provisioning, eliminating the need to repeat tasks such as entering a Wi-Fi Protected Setup PIN. Persistent Groups are accomplished by Wi-Fi Direct devices storing the Group information and credentials. Since Persistent Groups are invoked using Invitation signaling, all Wi-Fi Direct devices that support Persistent Groups must also support the Invitation mechanism.

Concurrent Connections and Multiple Groups

A Wi-Fi Direct Device that can be in a Group while maintaining a WLAN infrastructure connection at the same time is considered a Concurrent Device. For example, a laptop connected directly to a printer while simultaneously using a WLAN connection is operating as a Concurrent Device. Concurrent connections may be supported by a single radio and may support connections on different channels.

Concurrent operation requires support for multiple and distinct MAC entities, one for operation as a WLAN-STA and one for operating as a Wi-Fi Direct device. There are several approaches developers can take to implement multiple MAC entities. For example, maintaining two separate physical MAC entities, each associated with its own PHY entity, or using a single PHY entity encompassing two virtual MAC entities. These different approaches are beyond the scope of the P2P Specification.

Concurrent Devices may participate in multiple Groups simultaneously. The P2P Specification does not describe the mechanism for this capability – implementation is specific to the vendor.

Managed Environments

Operation in managed Wi-Fi environments (e.g. enterprise, hotspots, etc.) was an important consideration in the creation of the P2P Specification. To promote efficient use of wireless bandwidth, Wi-Fi Direct devices do not use 802.11b rates (1, 2, 5.5, or 11 Mbps) for data or management frames (barring Probe Request frames sent to both Wi-Fi Direct devices and Legacy Devices), nor shall they respond to requests indicating support only for 802.11b rates. This decreases the air time consumed by signaling between Wi-Fi Direct devices.

A WLAN AP may implement capabilities that allow it to manage Wi-Fi Direct devices, enabling robust protection and isolation of the enterprise infrastructure network. A WLAN AP with this capability may deauthenticate any Wi-Fi Direct device from the infrastructure network for out-of-policy behavior and communicate the reason for that action. For example, in an environment where controlled access to infrastructure network resources requires each device to authenticate, a P2P-enabled WLAN AP may communicate to all client devices that Cross-connection is not allowed. All Wi-Fi Direct devices are required to comply with this policy.

Wi-Fi Direct devices that implement optional Managed Device mechanisms can assist the WLAN AP in managing the Wi-Fi environment. A Managed Wi-Fi Direct device may aid the WLAN AP in gathering P2P co-existence information and the WLAN AP may signal channel or power limitations for P2P Groups. The WLAN AP may inform a Wi-Fi Direct device why it is being deauthenticated if it exhibits out-of-policy behavior, such as not managing coexistence in a fashion that reflects local IT requirements. Wi-Fi Direct devices report their identity to a WLAN AP when associating to enable such monitoring. While Managed device capabilities are optional to implement in WLAN APs and Wi-Fi Direct devices, enabled WLAN APs have the option of

authenticating only Managed devices (i.e., devices which support optional Managed mechanisms).

Certification Program Testing Overview

Certification plays an important role in providing consumers and businesses with confidence that Wi-Fi Direct devices will perform as expected, and that equipment from different vendors will interoperate seamlessly.

Only certified Wi-Fi Direct devices will be able to bear the Wi-Fi CERTIFIED Wi-Fi Direct word mark. To receive Wi-Fi Direct certification, a Wi-Fi Direct device must pass the following certification tests:

- **Baseline Wi-Fi certification tests:** Devices must support at least 802.11g as well as WPA2-Personal.
- **WMM and Wi-Fi Protected Setup certification tests:** Wi-Fi Multimedia (WMM) and Wi-Fi Protected Setup are optional Wi-Fi Alliance certifications, but both are mandatory for devices seeking Wi-Fi Direct certification.
- **All Mandatory certification tests:** These tests represent the minimum functionality Wi-Fi Direct devices must support.
- **Optional feature certification tests:** All optional features will be treated as "tested if implemented." This means that a) only devices supporting an optional feature will be tested for that feature and b) all devices supporting an optional feature must be tested for that feature.

The Wi-Fi Direct certification platform is comprised of member-contributed test bed devices (STAs and APs) and the Wi-Fi Alliance test automation platform (Sigma). The majority of test bed devices are STAs because of the mandatory requirement for Wi-Fi Direct devices to be capable of managing a Group. APs are used for coexistence, concurrence, and cross-connection testing purposes.

The software components of the Wi-Fi Alliance test automation platform are free to Wi-Fi Alliance members. It provides fully automated configuration of test bed devices as well as automated capture and analysis of sniffer traces. Client software comprised of a small-footprint Test Engine enables test automation on Devices Under Test (DUTs).

Figure 5 shows the architecture of the Wi-Fi Alliance test automation platform. A UCC (Unified CAPI Console) PC connects directly to the Device Under Test (DUT) or through a Control PC (i.e., such as connecting to a camera connected through a PC). Control PCs, if used, utilize the test network as a control network for Test Bed APs before and after testing. Each Control PC connects to one and only one device. A test bed STA may be any appropriate Wi-Fi Direct device with or without a Control PC.
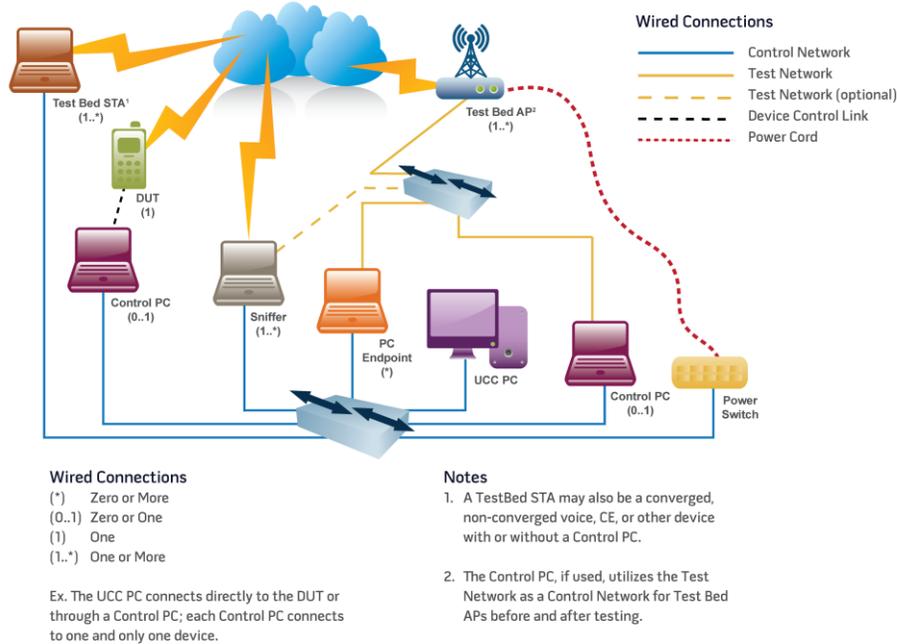
Sigma Test Automation Platform

Wired Connections

────────	Control Network
────────	Test Network
────────	Test Network (optional)
────────	Device Control Link
··········	Power Cord

Test Bed STA¹ (1..*)
DUT (1)
Control PC (0..1)
Sniffer (1..*)
PC Endpoint (*)
UCC PC
Control PC (0..1)
Power Switch
Test Bed AP² (1..*)

Wired Connections
(*)   Zero or More
(0..1) Zero or One
(1)   One
(1..*) One or More

Ex. The UCC PC connects directly to the DUT or through a Control PC; each Control PC connects to one and only one device.

Notes
1. A TestBed STA may also be a converged, non-converged voice, CE, or other device with or without a Control PC.

2. The Control PC, if used, utilizes the Test Network as a Control Network for Test Bed APs before and after testing.

Figure 5: Sigma Test Automation Platform Physical Architecture. The Wi-Fi Alliance test automation platform provides fully automated configuration of test bed devices as well as automated capture and analysis of sniffer traces.

Summary

The Wi-Fi Peer-to-Peer Specification expands the capabilities of Wi-Fi through support for direct connection between devices. Wi-Fi Direct devices offer the anytime, anywhere connectivity that users crave. Users can enjoy increased mobility and ease-of-use without sacrificing robust security and compatibility with legacy devices. Applications developers can leverage a powerful new set of capabilities to realize innovative applications and create future opportunities for manufacturers, content providers, and users.

Wi-Fi CERTIFIED Wi-Fi Direct™ devices make it more simple and convenient than ever to do things like print, share, sync and display - without joining a traditional home, office or hotspot network. Users can transfer content and share applications quickly and easily between mobile phones, cameras, printers, PCs and gaming devices. Wi-Fi Direct-certified devices also support connection with existing legacy Wi-Fi devices, bringing direct connection capabilities to the hundreds of millions of legacy Wi-Fi CERTIFIED devices already deployed.

Around the globe, more and more people are connecting digital devices in order to create and share content, download documents, music and videos, sync personal and work information and print photos, email, letters and documents. Wi-Fi Direct devices will be available to do the things they find most valuable in a direct connection - instant messaging, sharing pictures with friends and family, displaying those pictures from a portable device to a monitor or TV screen, video chatting, and playing video games with others.

Wi-Fi Direct devices greatly enhance the mobility and portability of content and applications across all of a user's devices using a single industry-wide technology, allowing users to access movies, music, and photos on-the-go. It also offers enhanced benefits of immediate connections,

ease of use and simple secure connections – enabling anytime, anywhere connectivity that users crave.

Wi-Fi has already changed the way the world connects. With Wi-Fi Direct, users will now find it even easier to share, show, print, and synchronize content however they want, wherever they are. With the next generation of Wi-Fi Direct devices, users will no longer need to think about connecting to the network because they are already carrying the network with them.

For more information about Wi-Fi Direct and other Wi-Fi CERTIFIED programs, a list of certified products, or a copy of the Wi-Fi Alliance Peer-to-Peer Specification, visit www.wi-fi.org/wi-fi_direct.php

About the Wi-Fi Alliance

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to the proliferation of Wi-Fi technology across devices and market segments. With technology development, market building, and regulatory programs, the Wi-Fi Alliance has enabled widespread adoption of Wi-Fi worldwide.

The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi enabled products deliver the best user experience. The Wi-Fi Alliance has completed more than 8,000 product certifications to date, encouraging the expanded use of Wi-Fi products and services in new and established markets.

Wi-Fi CERTIFIED™ makes it Wi-Fi: The Advantages of Choosing Wi-Fi CERTIFIED.

Since 2000, the Wi-Fi Alliance certification program has played a proactive, leading role in establishing interoperability among Wi-Fi equipment, enabling a great user experience, expanding Wi-Fi functionality, and improving the equipment's performance.

These efforts have been instrumental in widening the adoption of Wi-Fi and in making Wi-Fi CERTIFIED a globally known and trusted brand. When choosing a new device or access point, users look for the Wi-Fi CERTIFIED logo (Figure 6) and, for more detail, the Wi-Fi Interoperability Certificate (Figure 7), which gives them confidence that the product will work out of the box with Wi-Fi CERTIFIED equipment from any other vendor. Wi-Fi vendors worldwide send their products to be certified in one of the independent Wi-Fi Alliance Authorized Test Laboratories (ATLs).

To date, more than 8,000 product certifications have been completed. The recently introduced Wi-Fi CERTIFIED n certification program has been very successful, with more than 1,100 products certified since September 2009. The fastest growth is in mobile phones, with more than 100 Wi-Fi CERTIFIED models.

Wi-Fi certification programs meet the varying requirements of different device form factors, vendor choices, and market demand. Some Wi-Fi programs are mandatory, because they cover essential Wi-Fi features; others are optional.

Active Wi-Fi certification programs (asterisks indicate optional programs) include:

- **Interoperability and standard compliance:** IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n*

- **Security:** WPA2-Personal, WPA2-Enterprise* with EAP support, Wi-Fi Protected Setup*

- **Voice:** Voice-Personal*, Voice-Enterprise*

- **QoS and bandwidth management:** Wi-Fi Multimedia™ (WMM), WMM Admission Control*

- **Power conservation for mobile devices:** WMM Power Save*

- **Wi-Fi and cellular convergence:** Converged Wireless Group Radio Frequency (CWG-RF) Profile.

Figure 6. The Wi-Fi CERTIFIED logo found on the packaging of Wi-Fi equipment facilitates the user's selection.

Figure 7. The Wi-Fi Interoperability Certificate lists the capabilities and features supported by the AP or client device that have been tested by the Wi-Fi Alliance.

Figure 8. The Wi-Fi CERTIFIED product database is available online at **www.wi-fi.org**