Wi-Fi CERTIFIED™ TDLS:

Easy-to-use, security-protected direct links to improve performance of Wi-Fi® devices

Wi-Fi Alliance®
August 2012

Executive Summary

Wi-Fi CERTIFIED™ TDLS, or Tunneled Direct Link Setup, is a certification program for devices implementing technology enabling them to connect directly to one another after they have joined a traditional Wi-Fi® network. Products bearing the Wi-Fi CERTIFIED TDLS designation can set up secure links with each other and transfer data directly between them. TVs, smartphones, cameras, printers, PCs, projectors, and gaming devices, for example, will be able to connect directly to each other to transfer content and share applications quickly and easily.

The establishment of direct links between TDLS-certified devices requires no user intervention. Wi-Fi TDLS products are based upon the IEEE 802.11z standard amendment. They have been tested and certified for this technology in addition to core interoperability and current-generation WPA2™ security**.**

In the home and enterprise environments, TDLS technology greatly enhances the efficiency of communication between different devices in a network, such as streaming (video and audio), data migration and data backup.

This white paper provides a detailed look at the TDLS certification program and the benefits of the technology.

Introduction

Today, roughly 17 percent of all people in the world use Wi-Fi to stay connected[1]. More than 1 billion Wi-Fi devices were shipped in 2011[2]. Wi-Fi is widely available in homes, Wi-Fi hotspots, and enterprise environments, and is found in many types of devices, including notebook computers, cameras, media players, TVs, gaming devices, and mobile phones. In parallel to this expansion of device types, the number of demanding applications has increased, and the overall volume of content transmitted over typical Wi-Fi networks has exploded.

Wi-Fi CERTIFIED TDLS is an important innovation in Wi-Fi to keep pace with the evolving requirements of Wi-Fi usage. TDLS optimizes performance by establishing a direct link between devices so that they can more efficiently complete tasks such as streaming multimedia, transferring files, or backing up data. TDLS links require no user intervention to set up, and automatically support the highest-available level of security. The use of TLDS links almost always results in increased capacity on the overall network.

TDLS is based on the IEEE 802.11z standard amendment. TDLS is characterized by the use of set-up frames that are encapsulated in data frames that can be transmitted through the access point (AP) transparently. This is known as 'tunneling' the frame through the AP. The result of this tunneling action is that direct connections can be formed in a Wi-Fi network without a requirement for special functionality in the AP. Wi-Fi TDLS devices can set up direct links providing improved speed of connection and overall bandwidth efficiency.

---

[1] ABI Research, 2012
[2] ABI Research, 2012

Wi-Fi CERTIFIED TDLS is an optional certification program for client devices such as smartphones, laptops, and set top boxes. Devices bearing the Wi-Fi CERTIFIED TDLS designation have completed testing to validate that they have implemented the program's features in an interoperable fashion.

Wi-Fi CERTIFIED TDLS: Key Benefits

The use of TDLS links makes data transmission more efficient. In a typical infrastructure Wi-Fi network, packets that are communicated between two devices are sent via the AP. The first device will send the packet to the AP and the AP then forwards that packet to the second device. In this model, two data packets are transmitted over the medium to deliver just one data packet from one device to another. However, if two devices are within communication range of one another, then a direct link can reduce by half the number of packet transmissions. Such links increase the efficiency of the network, especially if the two devices are relatively closer to each other than to the AP.

TDLS links enable devices to perform at the highest level of shared capabilities, regardless of the capabilities of the AP. In the setup process, devices exchange their capabilities. If both devices support more advanced capabilities than the AP, then the communication on the direct link can be at this higher level. For example, if the AP only supports 802.11g and the two TDLS devices support 802.11n, then the devices can communicate at higher 802.11n data rates over the direct link.

In addition, TDLS also provides support for devices to negotiate an alternative channel. For example, if the two TDLS-linked devices are dual-band they may choose to dynamically switch to a 40MHz 802.11n channel in the 5 GHz band. The net result is a significant improvement in performance, latency and network capacity.

Individual TDLS-linked devices maintain full access to the Wi-Fi network. Even when the direct link is switched to another channel, the stations periodically switch back to the home channel to maintain the connectivity with the Wi-Fi network. The AP is unaware of the TDLS setup and no functionality is required to support the link. TDLS can be used with all existing and new APs.

TDLS link setup does not require user intervention. Because devices negotiate and establish a TDLS link automatically, even non-technical users will be able to benefit from the technology. A device uses the TDLS discovery procedure to measure the signal strengths from candidate TDLS devices, which can aid in deciding whether to set up a TDLS link.

TDLS-linked devices support WPA2 security, regardless of the overall security level of the network. As long as the network is using some form of security, the TDLS direct link always employs WPA2 encryption even if the network is using a lower encryption. The keys are automatically exchanged during the TDLS setup procedure so no user password is required.

TDLS can operate within a Wi-Fi CERTIFIED Wi-Fi Direct™ network. Wi-Fi Direct networks are device-to-device networks in which a single device acts as a "Group Owner" and no traditional AP or internet connection is required. TDLS links can be established between two devices that are communicating to a Group Owner (GO) on a Wi-Fi Direct connection.   In this case, the link is activated the same way as in a Wi-Fi network, only the GO acts as the AP in that situation.

TDLS Use Cases

TDLS devices provide an enhanced user experience to both consumers and enterprise users. The following examples illustrate how users will benefit from TDLS functionality without having to intervene to activate the feature.
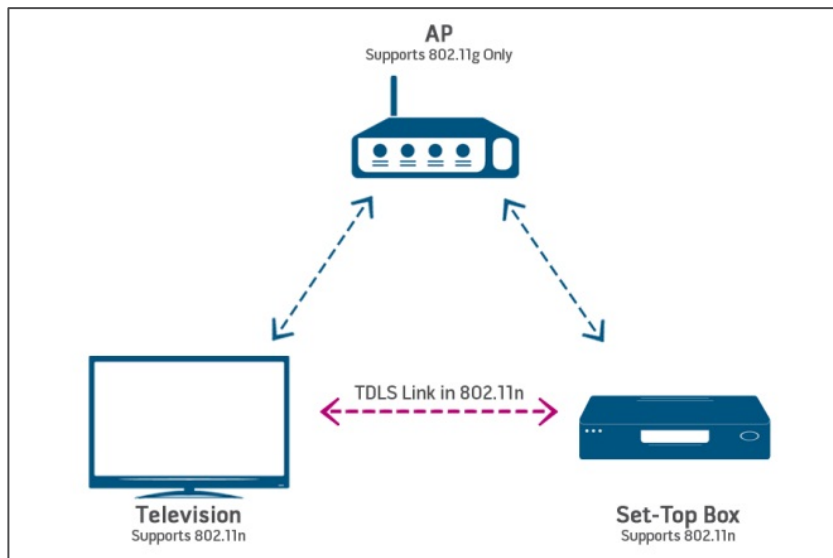
Streaming media to a Wi-Fi TV

Joe has a movie stored on his tablet (or smartphone) which he wants to view on his TV. The TV and the tablet are connected to the home Wi-Fi network. The TV and the tablet are in the same room downstairs, while the AP is located upstairs. Joe starts the movie, and the tablet and the TV automatically set up a TDLS link. This results in the fastest possible connection and improves the overall efficiency of the home network.

Similarly, the movie might have been on a Network Attached Storage (NAS) Device Drive or a Set-Top Box streaming to the TV. In each case the TDLS link is set up automatically.

Figure 1 illustrates this use case. Note that although the AP is an 802.11g device, the two TDLS-linked devices support 802.11n and are able to communicate at the higher data rate provided by that standard.


Fig. 1: Streaming Media to a Wi-Fi TV

Transfer of files from a PC to a smartphone

Sally has loaded a series of videos on her home PC. She wants to transfer this content to her smartphone for viewing during a plane ride.

Sally's smartphone always automatically connects to the home AP as soon as she enters her home. The PC, located in the home office, is also associated with the home AP. The AP is located in the living room. On her smartphone, Sally selects the video content to be downloaded from her home PC. Typically, she sets the
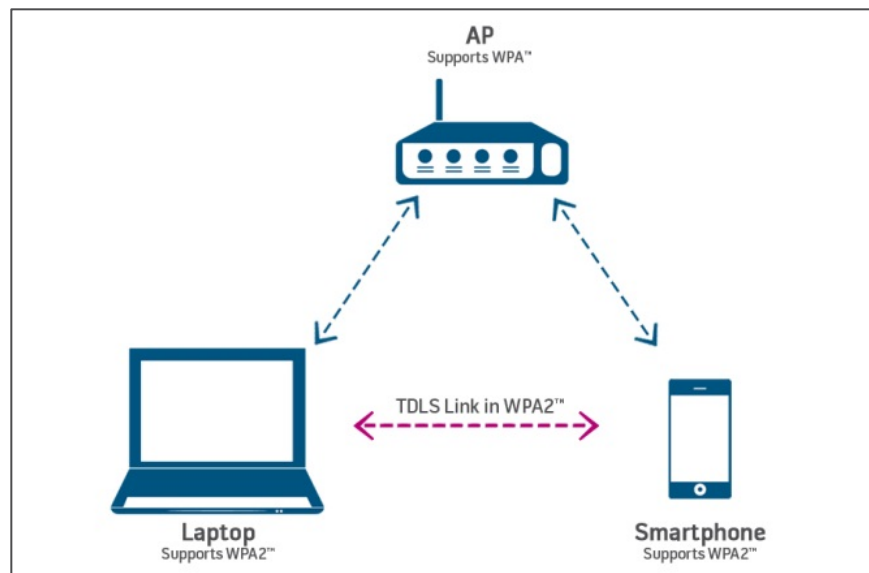
Fig. 2: Transfer of Files from a PC to a Smartphone

smartphone down next to her PC in the home office while she downloads content.

The smartphone and the home PC automatically negotiate a TDLS link to offload the utilization of the home Wi-Fi network to reduce the time it takes to download the video content.

Figure 2 illustrates this use case. Note that although the AP supports only WPA, an older form of Wi-Fi security, the smartphone and PC are able to form a link protected by WPA2, the current form of Wi-Fi security, since both devices support that feature.

Streaming to a Wi-Fi speaker

Kevin has a set top box that has access to music stations. The set top box is in the lounge. When working in his study he likes to listen to the music channels, where he has installed Wi-Fi speakers. The set top box and the Wi-Fi speakers are connected to the home Wi-Fi network. Kevin sets up the desired music channel on the set top box and streams the music to his speakers in the study. The set top box and the Wi-Fi speakers automatically set up a direct link, improving the efficiency of the home network.

Wireless Printing in a Wi-Fi Direct Network

Kumar has returned from a camping trip, where he took several pictures on his smartphone. He comes home and is eager to print them on his Wi-Fi-enabled printer. The laptop and printer are connected using Wi-Fi Direct, and the laptop is acting as the GO.

Kumar's smartphone automatically joins the laptop's Wi-Fi Direct network, since they have been previously provisioned. Kumar launches a photo viewing application on his smartphone, selects several pictures, and clicks "print". The smartphone and printer negotiate a direct link session to avoid going through the GO. This improves efficiency in the Wi-Fi Direct group network and streamlines data transmission between the smartphone and the printer. The TDLS-linked devices also take advantage of TDLS power-save capabilities, to conserve the smartphone's battery.
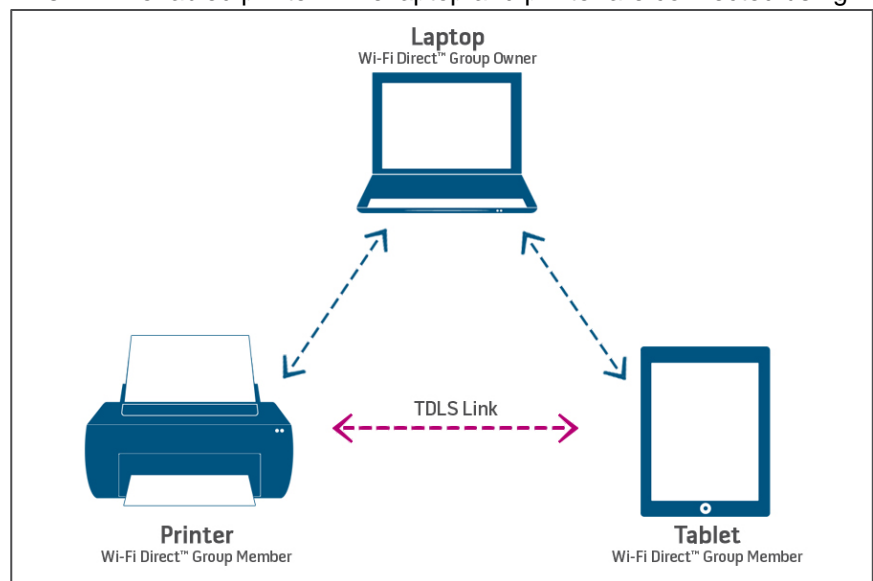
**Fig. 3: Wireless Printing in a Wi-Fi Direct Network**

Figure 3 illustrates this use case.

Wireless Data Back Up

After being away from his home network due to travel, Hong needs to back up his laptop. The laptop is connected to his home AP, and the backup application discovers the storage device on the network and begins operation. The laptop and storage device negotiate a direct link session to avoid the additional hop through the home AP, and to operate on a 40 MHz channel in 5 GHz, which is not supported by the home AP.

Figure 4 illustrates this use case.
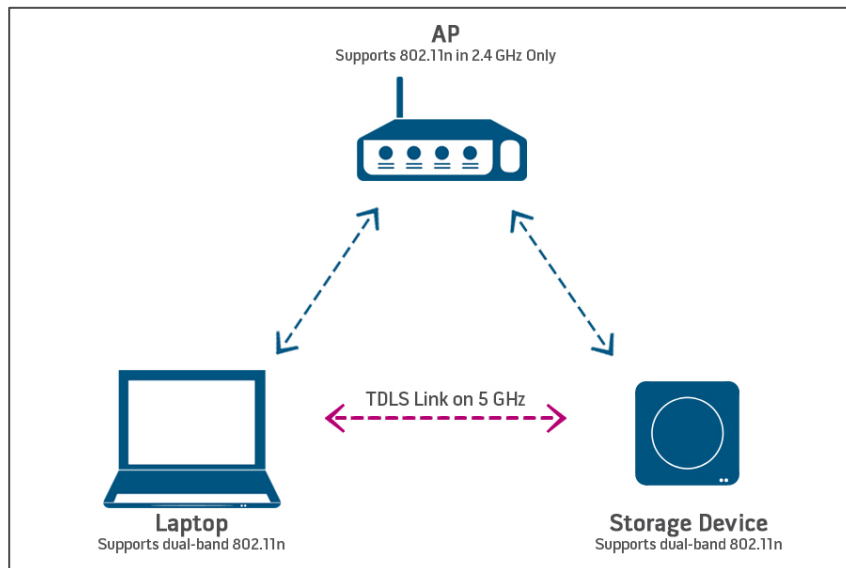
Fig. 4: Wireless Data Back Up

How does Wi-Fi CERTIFIED TDLS work?

The key processes used in Wi-Fi CERTIFIED TDLS are Discovery, Setup, Teardown, Power Save, and Channel Switch, and they are described in detail below. TDLS security features are also described in this section.

TDLS Discovery

The TDLS Discovery process begins when one TDLS device sends a TDLS Discovery request to another device, via the AP or GO. If the target device is also TDLS compliant, then it sends a TDLS discovery response directly to the initiator, providing information on its capabilities, including supported rates and channels. In addition to providing the information that the intended target does indeed support TDLS, the TDLS Discovery frame exchange may be used to measure the relative signal strengths of the AP and candidate TDLS device. This would inform a decision on whether a direct link would be beneficial. By comparing the received signal strength from the target device to that from the AP, the initiating device can assess if a direct link will be more efficient than sending the packets via the AP.

Note that the use of the TDLS Discovery exchange is not required. A TDLS device may choose to simply attempt a TDLS Setup.

TDLS Setup and Teardown

A series of frame exchanges is used to set up a TDLS link. The initiating device first sends a TDLS Setup request, tunneled through the AP, to the target device. This frame includes information about the capabilities of the requesting device. The target device then responds with the TDLS Setup response, also tunneled through the AP, including information about its capabilities plus a status code that either

accepts or rejects the setup request. If the Setup Request is accepted, the initiating device then sends the TDLS Confirm Frame via the AP. At this point the devices begin to communicate directly.

Either the requesting or accepting device may send a TDLS Teardown Frame directly to the other device or, if unreachable, this frame can be tunneled via the AP.

TDLS Power Save

The TDLS Peer Power Save scheme is similar to WMM®-Power Save, also known as WMM U-APSD, where packets intended for a device that is sleeping are buffered until the device is awake. In TDLS certification testing, the ability to be a TDLS Peer U-APSD buffer device is mandatory, whereas the ability to sleep is optional.

When the buffer device is always awake, the action is very similar to that of WMM U-APSD. The actions are as follows:

1. TDLS peer buffer device buffers packet(s) for the sleeping device

2. Buffer device sends a TDLS peer traffic indication frame addressed to the sleeping device, via the AP

3. AP will set the Traffic Indication Map (TIM) for the sleeping device in the beacon, informing the sleeping device that there is traffic buffered

4. The sleeping device wakes for beacon, notes TIM and triggers the AP to send the TDLS peer traffic indication frame

5. The now-awake device then sends a TDLS peer traffic response frame directly to the buffer device, which initiates a service period between the two devices

6. The buffer device sends the buffered packet(s) directly to the receiving device

7. When the buffer device indicates that no more packets are buffered, the receiving device may go back to sleep

It is also possible for both TDLS devices to enter power save mode and both sleep. In this case, both stations operate as buffer devices and buffer traffic for their peer. The procedure is similar to that described above, except that at Step 2), after sending the TDLS peer traffic indication frame to the AP, the device stays awake until it receives the TDLS peer traffic response frame. Then it will send the buffered traffic, after which it may return to the sleep mode.

Note that as the announcement of buffered packets is always carried out by the AP, the TDLS-linked devices are still able to communicate with other devices in the same network.

TDLS Channel Switch

TDLS devices can negotiate to move to another channel. For example, if the network is operating in a congested 2.4 GHz channel as its base channel, and the two TDLS devices advertise in the TDLS setup request or response that they both support 5 GHz channels, then it may be advantageous to move to a 5 GHz channel, as an off channel.

Before moving from the base channel to an off channel, the TDLS devices inform the AP that they are in 'sleep mode,' so that the AP will buffer packets. When operating via the off channel, the TDLS devices regularly return to the base channel in order to receive beacons, look at the TIM for any buffered packets, and communicate with other devices in the network. When using an off channel, the TDLS devices are not permitted to sleep.

The basic procedure for the TDLS channel switch is as follows:

1. The originator TDLS device enters power save with the AP, and sends a TDLS Channel Switch request to a second TDLS device. This request includes the target channel information.

2.   The second TDLS device enters power save with the AP and sends a TDLS Channel Switch response, which includes the status code 0 (accepted) and confirms the target channel as the desired off channel

3.   Both devices then switch from the base channel to the off channel. Data must flow via the off channel before a set switch timeout. If no data flows before this timeout, then the devices return to the base channel.

4.   When using the off channel, either device may send an unsolicited TDLS channel switch response to its peer with the base channel as the target. The peer device will respond with an ACK, and the devices return to the base channel.

5.   Both devices will switch back to base channel periodically to listen to AP beacons and possibly communicate with network devices

In an enterprise environment, where the channel allocations and loading is centrally controlled, the administrator may wish to exclude channel switching and therefore a "TDLS Channel Switching Prohibited" bit may be set in the AP beacon.

TDLS Security Features

When setting up a TDLS link, the security for that link is always set to WPA2 encryption, unless the network is using an open, non-secured configuration, in which case the direct link is also set to open. The setup frame exchanges include the security key exchanges, such that the security domain for the direct link is unique – distinct from the network's overall security domain. No user password is required to be entered.

TDLS capability can be disabled by a system administrator. In an enterprise environment, for example, a system administrator may wish to exclude direct links and therefore a "TDLS Prohibit" bit may be set in AP beacons.

Wi-Fi CERTIFIED Interoperability Certificate

Wi-Fi CERTIFIED™ Interoperability Certificate

Certification ID: WFAxxxxx

This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification programs is available at www.wi-fi.org/certification_programs.php.

Certificate Date:	date_of_last_product_certification
Company:	company_name
Product:	product_name
Model/SKU#:	model_number/sku
Primary Category:	primary_product_category

Tested Spatial Streams	Dual-Band Concurrent 2.4GHz	5GHz
Transmit	3	3
Receive	3	3

IEEE Standard

IEEE 802.11a
IEEE 802.11b
IEEE 802.11d
IEEE 802.11g
IEEE 802.11h
IEEE 802.11n

Optional 802.11n Capabilities
- Short Guard Interval
- Greenfield Preamble
- TX A-MPDU
- STBC
- 40 MHz operation in 2.4 GHz with coexistence mechanisms
- 40 MHz operation in 5 GHz
- HT Duplicate (MCS 32)

Security

WPA™ - Enterprise/Personal
WPA2™ - Enterprise/Personal
Protected Management Frames

EAP Type(s)
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP-AKA
EAP-FAST

Vendor EAP Type(s)
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP-AKA
EAP-FAST

Multimedia

WMM®
WMM®-Power Save
WMM® -Admission Control
TDLS

Convergence

Voice – Personal
Voice – Enterprise

CWG-RF

Special Features

Wi-Fi Protected Setup™
- PIN
- PBC
- Internal Registrar (APs only)
- External Registrar support options

Wi-Fi Direct™

IBSS with Wi-Fi Protected Setup

For more information: www.wi-fi.org/certification_programs.php

Fig. 5: Wi-Fi CERTIFIED interoperability certificate

Every Wi-Fi CERTIFIED product holds a certificate (sample above) issued by the Wi-Fi Alliance. An indication that a device has successfully passed testing for the TDLS certification program will be indicated in the Interoperability Certificate as a bullet under the Multimedia column.

An interoperability certificate is available for each product that is Wi-Fi CERTIFIED. The interoperability certificate indicates the certification programs supported by a Wi-Fi device. Depending on the deployment and application needs, different certifications are required.

Conclusions and Additional Resources

The Wi-Fi CERTIFIED TDLS program supports an important new innovation in Wi-Fi technology. The ability of devices to transparently negotiate and establish a direct link, without user intervention, will improve the overall user experience with Wi-Fi technology, especially when using advanced applications like multimedia streaming.

The use of TDLS can improve overall network capacity. TDLS links deliver a more efficient, higher-performing connection between linked devices, and help ensure that linked devices are protected with WPA2 security when part of a security-protected Wi-Fi network. Power-saving mechanisms extend TDLS' benefits when using battery-operated devices. The ability to form TDLS links is defined by the presence of two or more TDLS-certified devices, and does not require that an AP provide special functionality.

For additional reading, please see the following documents:

Wi-Fi CERTIFIED™ for WMM®-Power Save: Support for Advanced Power Save for Mobile and Portable Devices in Wi-Fi® Networks (Wi-Fi Alliance, 2005)

Wi-Fi CERTIFIED™ n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks (Wi-Fi Alliance, 2009)

Wi-Fi CERTIFIED Wi-Fi Direct™: Personal, Portable Wi-Fi® Technology (Wi-Fi Alliance, 2010)

About the Wi-Fi Alliance

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to seamless connectivity. 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 15,000 product certifications, encouraging the expanded use of Wi-Fi products and services in new and established markets.

Wi-Fi®, Wi-Fi Alliance®, WMM®, Wi-Fi Protected Access® (WPA), the Wi-Fi CERTIFIED logo, the Wi-Fi logo, the Wi-Fi ZONE logo and the Wi-Fi Protected Setup logo are registered trademarks of the Wi-Fi Alliance. Wi-Fi CERTIFIED™, Wi-Fi Direct™, Wi-Fi Protected Setup™, Wi-Fi Multimedia™, WPA2™, Wi-Fi CERTIFIED Passpoint™, Passpoint™, Wi-Fi CERTIFIED Miracast™, Miracast™, Wi-Fi ZONE™ and the Wi-Fi Alliance logo are trademarks of the Wi-Fi Alliance.

Acronyms

AP	Access Point
GO	Group Owner
TDLS	Tunneled Direct Link Setup
TIM	Traffic Indication Map