Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14237
Date:	2010-02-25
Replaces:	
Document Type:	Liaison organization contribution
Document Title:	Liaison Statement from IEEE 802.11 WG to ISO/IEC JTC 1/SC 6 on the IEEE P802.11z™/D7.0
Document Source:	IEEE 802.11 WG
Project Number:	
Document Status:	SC 6 NBs are requested to submit comments on this draft to SC 6 Secretariat by 2010-03-19 to forward them for consideration to the IEEE 802.11 WG.
Action ID:	COM
Due Date:	2010-03-19
No. of Pages:	90

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

IEEE P802.11z™/D7.0

Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

Amendment 6: Extensions to Direct Link Setup (DLS)

Prepared by the 802.11 Working Group of the
IEEE 802 Committee

IEEE Standards Activities Department
445 Hoes Lane
Piscataway, NJ 08854, USA

Abstract: This amendment provides Direct Link Setup enhancements to the IEEE 802.11 MAC and PHY, extending direct link setup to be independent of the access point (AP), and adding power save capabilities. The direct link setup is made independent of the AP by tunneling the protocol messages inside data frames.

Keywords: Direct Link, Power Saving

This page is left blank intentionally.

Introduction

(This introduction is not part of IEEE P802.11z/D7.0, Draft Standard for Information Technology – Telecommunications and information exchange between systems - Local and metropolitan area networks – Specific requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications. Amendment 6: Extensions to Direct Link Setup)

This document provides amendments to the IEEE 802.11 PHY/MAC layers related to direct link setup.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this draft amendment to standard was completed, the IEEE 802.11 Working Group had the following membership:

Bruce Kraemer, Chair

Adrian Stephens and Jon Rosdahl, Vice-chairs

Stephen McCann, Secretary

EDITORIAL NOTE—a three column list of voting members of 802.11 on the day the draft was sent for sponsor ballot will be inserted

The following were officers of Task Group z:

Menzo Wentink, Chair
Daniel Borges, Secretary
Menzo Wentink, Technical Editor

Major contributions were received from the following individuals:

Adrian Stephens
Alexander Safonov
Ali Raissinia
Ashish Shukla
Bas Driesen
Daniel Borges
David Hunter
Ding Zhiming
Eunha Kim
Ganesh Venkatesan
Graham Smith
Guiming Shu
Harish Ramamurthy
Harry Worstell
Henry Ptasinski
Jakub Majkowski
Jari Jokela
Jarkko Kneckt
Jesse Walker
Jiyoung Huh
Junghoon Jee
Junling Hu
Kapil Sood
Kevin Hayes
Leo Estevez
Liwen Chu
Marc Jalfon
Matthew Fischer
Menzo Wentink
Michael Livshitz
Michael Montemurro
Michelle Gong
Qi Wang
Ray Hayes
Shravan Surineni
Shu Guiming
Sihoon Yang
Simon Barber
Srinivasa Duvvuri
Suman Sharma
Yeonkwon Jeong
Yongho Seok

The following members of the balloting committee voted on this Standard. Balloters may have voted for approval, disapproval, or abstention.

EDITORIAL NOTE—a three-column list of responding sponsor ballot members will be inserted by IEEE staff

Editorial Notes

EDITORIAL NOTE—Two forms of editorial markup are used: Notes and Comments. Editorial Notes and Editorial Comments are not part of the amendment and will be removed before it is published, together with any other contents in this subclause. This paragraph is an example of how an Editorial Note is marked. Editorial Comments are marked (Ed:), and contain references to submissions or comment resolutions to track the origin of changes.

EDITORIAL NOTE—Headings with empty content or Headings preceding editing instructions that modify the contents of the referenced subclause are there to provide context to the reader of this document, they have no other significance.

Table of Contents

List of figures

List of tables

IEEE P802.11z™/D7.0

Draft STANDARD for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

Amendment 6: Extensions to Direct Link Setup (DLS)

(This amendment is based on IEEE Std 802.11™–2007, as amended by 802.11k™-2008, 802.11r™-2008, 802.11y™-2008, 802.11w™-2009, 802.11n™-2009

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: ***change, delete, insert, and replace***. Change is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

2. Normative references

Insert the following new reference in alphabetical order:

IETF RFC 1042, A Standard for the Transmission of IP Datagrams over IEEE 802 Networks, J. Postel, J. Reynolds, February 1988.

3. Definitions

EDITORIAL NOTE—The subclause numbering of definitions is of the form "3.z<x>" where <x> is an increasing number. The 802.11 technical editor will assign numbers when merging this list into the baseline document.

Change definition 3.45 as follows:

3.45 dynamic frequency selection (DFS) owner: A station (STA) in an independent basic service set (IBSS) or off-channel TDLS direct link that takes responsibility for selecting the next channel after radar is detected operating in a channel. In an IBSS, it cannot be guaranteed that there will be a single DFS owner at any particular time and the protocol is robust to this situation.

Insert new definitions 3.z1 through 3.z14 retaining the alphabetic ordering:

3.z1 tunneled direct link setup (TDLS): A protocol that uses a specific Ethertype encapsulation to tunnel direct link setup frames through an AP to establish a TDLS direct link. TDLS is separate from direct link setup (DLS).

3.z2 TDLS initiator STA: A STA that transmits a TDLS Setup Request frame or a TDLS Discovery Request frame.

3.z3 TDLS responder STA: A STA that receives or is the intended recipient of a TDLS Setup Request frame or TDLS Discovery Request frame.

3.z4 TDLS peer STA: STA with a TDLS direct link.

3.z5 peer unscheduled automatic power save delivery (Peer U-APSD): A power save mode based on unscheduled service periods that may be used between two STAs that have set up a TDLS direct link.

3.z6 TDLS peer power save mode (TDLS Peer PSM): A power save mode that is based on periodically scheduled service periods, which may be used between two STAs that have set up a TDLS direct link.

3.z7 TDLS Peer PSM initiator: A STA that transmits a TDLS Peer PSM request frame.

3.z8 TDLS Peer PSM responder: A STA that transmits a TDLS Peer PSM response frame.

3.z9 peer U-APSD (PU) sleep STA: A TDLS peer STA that entered power save mode on a TDLS direct link and that is using Peer U-APSD for the delivery of buffered traffic.

3.z10 PU buffer STA: A TDLS peer STA that buffers traffic for a PU sleep STA.

3.z11 TDLS direct link: Direct link between two non-AP STAs that has been established using the TDLS protocol.

3.z12 TDLS power save mode: TDLS Peer PSM or Peer U-APSD.

3.z13 Base channel: Channel on which the TDLS peer STA is associated with an AP.

3.z14 Off-channel: Channel that is not the base channel.

3.z15 AP Path: Path between two TDLS peer STAs via the AP.

3A. Definitions specific to IEEE 802.11

Change definition 3A.26 as follows:

3A.26 IDO STA: a STA that is the DFS Owner of an IBSS or off-channel TDLS direct link that is operating on a channel within a regulatory class that has a value of 20 or 40 for the entry in the column labeled "Channel Spacing (MHz)" and that has a value of 5 for the entry in the column labeled "Channel Starting Frequency (GHz)" of any of the tables found in Annex J.

4. Abbreviations and acronyms

Insert the following new abbreviations and acronyms into Clause 4, while maintaining alphabetic ordering:

IE	Information Element
TDLS	Tunneled Direct Link Setup
TPK	TDLS Peer Key
TPKSA	TDLS Peer Key Security Association
TDLS Peer PSM	Tunneled Direct Link Setup Peer Power Save Mode
Peer U-APSD	Peer Unscheduled Automatic Power Save Delivery
PU	Peer U-APSD
PTI	Peer Traffic Indication

5. General description

5.2 Components of the IEEE 802.11 architecture

Insert the following new subclause after 5.2.9 and its subclauses, if any:

5.2.10 Tunneled Direct Link Setup

Tunneled Direct Link Setup (TDLS) is characterized by the use of signaling frames that are encapsulated in data frames so that the signaling frames can be transmitted through an AP transparently. Therefore, unlike with DLS, the AP does not need to be direct link aware, nor does it have to support the same set of capabilities that will be used on the direct link, in order for TDLS to be used. To allow a STA to enter a TDLS power save mode, TDLS provides two power save mechanisms: Peer U-APSD and TDLS Peer PSM. TDLS allows STAs to use the TDLS Peer Key handshake to provide data confidentiality and

message authentication. STAs that set up a TDLS direct link remain associated with the AP, but have the option of transmitting frames directly to the other TDLS peer STA. TDLS is separate from DLS.

7. Frame formats

7.1 MAC frame formats

7.1.3 Frame fields

7.1.3.1 Frame Control field

7.1.3.1.7 More Data field

Insert the following paragraph at the end of 7.1.3.1.7:

If a STA with TDLS Peer PSM enabled sets the More Data Ack subfield to one in its QoS Capability information element of its transmitted TDLS Setup Request frame or TDLS Setup Response frame, then a TDLS peer STA may indicate that it has a pending transmission for the STA by setting the More Data field to one in ACK frames transmitted to the STA.

7.1.3.5 QoS Control field

Change Table 7-4 as shown:

Table 7-4—QoS Control field

Applicable Frame (sub) Types	Bits 0-3	Bit 4	Bits 5-6	Bit 7	Bits 8-15
QoS CF-Poll and QoS CF-Ack+ CF-Poll frames sent by HC	TID	EOSP	Ack Policy	Reserved	TXOP limit
QoS Data+CF-Poll and QoS Data+CF-Ack+CF-Poll frames sent by HC	TID	EOSP	Ack Policy	A-MSDU Present	TXOP limit
QoS Data and QoS Data+CF-Ack frames sent by HC	TID	EOSP	Ack Policy	A-MSDU Present	AP PS Buffer State
QoS Null frames sent by HC	TID	EOSP	Ack Policy	Reserved	AP PS Buffer State
QoS Data and QoS Data+CF-Ack frames sent by non-AP STAs that are not a PU buffer STA or a PU sleep STA	TID	0	Ack Policy	A-MSDU Present	TXOP duration requested
	TID	1	Ack Policy	A-MSDU Present	Queue size
QoS Null frames sent by non-AP STAs that are not a PU buffer STA or a PU sleep STA	TID	0	Ack Policy	Reserved	TXOP duration requested
	TID	1	Ack Policy	Reserved	Queue size
QoS Data and QoS Data+CF-Ack frames sent by PU buffer STAs	TID	EOSP	Ack Policy	A-MSDU Present	Reserved
QoS Null frames sent by PU buffer STAs	TID	EOSP	Ack Policy	Reserved	Reserved
QoS Data and QoS Data+CF-Ack frames sent by PU sleep STAs	TID	Reserved	Ack Policy	A-MSDU Present	Reserved
QoS Null frames sent by PU sleep STAs	TID	Reserved	Ack Policy	Reserved	Reserved

7.3 Management frame body components

7.3.1 Fields that are not information elements

7.3.1.7 Reason Code field

Insert two new reason codes into Table 7-22, and update the reserved values accordingly:

Table 7-22—Reason codes

Reason code	Meaning
25	TDLS direct link teardown due to TDLS peer STA unreachable via the TDLS direct link
26	TDLS direct link teardown for unspecified reason

7.3.1.9 Status Code field

Insert six new status codes into Table 7-23, and update the reserved values accordingly:

Table 7-23—Status codes

Status code	Meaning
2	TDLS wakeup schedule rejected but alternative schedule provided
3	TDLS wakeup schedule rejected
4	Direct links not allowed by the BSS
5	Security disabled
6	Unacceptable lifetime
7	Not in same BSS
70	Unexpected message
71	Invalid SNonce
72	Invalid contents of RSNIE

7.3.1.11 Action field

Insert one new row (ignoring the header row) in Table 7-24 in the correct position to preserve ordering by the "Code" column, and update a "Reserved" range of values appropriately.

Table 7-24—Category Values

Code	Meaning	See subclause
12	TDLS	7.4.11

7.3.2 Information elements

In table 7-26, insert five new information elements, and renumber the reserved values accordingly:

Table 7-26—Element IDs

Information element	Element ID	Length (in octets)	Extensible
Link Identifier (see 7.3.2.61)	101	20	Yes
Wakeup Schedule (see 7.3.2.62)	102	12	Yes
Channel Switch Timing (see 7.3.2.63)	104	6	Yes
PTI Control (see 7.3.2.64)	105	5	Yes
PU Buffer Status (see 7.3.2.65)	106	3	Yes

7.3.2.25 RSN information element

7.3.2.25.2 AKM suites

Insert one new entry in Table 7-34 and update the reserved values accordingly:

Table 7-34—AKM suite selectors

OUI	Suite type	Authentication type	Key management type
00-0F-AC	7	TDLS	TPK Handshake

7.3.2.27 Extended Capabilities information element

Insert three new rows to Table 7-35a as follows and renumber the reserved values accordingly:

Table 7-35a—Capabilities field

Bit	Information	Notes
28	TDLS Support	The TDLS Support subfield indicates support for TDLS, as defined in 11.19. When dot11TunneledDirectLinkSetupImplemented is true, this field is set to one to indicate support for TDLS. The field is set to zero otherwise, to indicate that TDLS is not supported,
29	Peer U-APSD Buffer STA Support	The Peer U-APSD Buffer STA Support subfield indicates support for the Peer U-APSD Buffer STA function, as defined in 11.2.1.14. When dot11TDLSPeerUAPSDBufferSTAActivated is true, and to indicate support for Peer U-APSD on this link, the Peer U-APSD Buffer STA Support subfield is set to one. Otherwise, the Peer U-APSD Buffer STA Support subfield is set to zero to indicate that this capability is not supported on this link.
30	TDLS Peer PSM Support	The TDLS Peer PSM Support subfield indicates support for TDLS Peer PSM, as defined in 11.2.1.13. When dot11TDLSPeerPSMActivated is true, and to indicate support for TDLS Peer PSM on this link, the TDLS Peer PSM Support subfield is set to one. Otherwise, the TDLS Peer PSM Support subfield is set to zero to indicate that this capability is not supported on this link.
31	TDLS channel switching	When dot11TDLSChannelSwitchingActivated is true, and to indicate that the STA supports Tunneled Direct Link Setup (TDLS) with TDLS Channel Switching on this link as described in 11.19, the TDLS Channel Switching capability subfield is set to one. Otherwise, the TDLS Channel Switching subfield is set to zero to indicate that this capability is not supported on this link.
32	TDLS Prohibited	The TDLS Prohibited subfield indicates whether the use of TDLS is prohibited. The field is set to one to indicate that TDLS is prohibited, and to zero to indicate that TDLS is allowed.
33	TDLS Channel Switching Prohibited	The TDLS Channel Switching Prohibited subfield indicates whether the use of TDLS Channel Switching is prohibited. The field is set to one to indicate that TDLS Channel Switching is prohibited, and to zero to indicate that TDLS Channel Switching is allowed.

Insert new subclauses 7.3.2.61 through 7.3.2.65 after subclause 7.3.2.60:

7.3.2.61 Link Identifier element

The Link Identifier element contains information that identifies a TDLS direct link. The element information format is defined in Figure 7-95o28.

	Element ID	Length	BSSID	TDLS initiator STA Address	TDLS responder STA Address
Octets:	1	1	6	6	6

Figure 7-95o28—Link Identifier element format

The Length field is set to 18.

The BSSID field is set to the BSSID of the BSS to which the TDLS initiator STA is associated.

The TDLS initiator STA Address field is set to the TDLS initiator STA's MAC address.

The TDLS responder STA Address field is set to the TDLS responder STA's MAC address.

7.3.2.62 Wakeup Schedule information element

The Wakeup Schedule information element contains information regarding the periodic wakeup schedule for TDLS Peer Power Save Mode. The information element format is defined in Figure 7-95o29.

	Element ID	Length	Offset	Interval	Awake Window Backoff	Awake Window Duration	Idle Count
Octets:	1	1	4	4	4	2	2

Figure 7-95o29—Wakeup Schedule element format

The Length field is set to 10.

The Offset field is the time in microseconds between TSF 0 and the start of a first Awake Window. See 11.2.1.13.

The Interval field is set to the time in microseconds between the start of two successive Awake Windows. See 11.2.1.13.

The Awake Window Backoff field is set to the duration of the Awake Window, in units of backoff slots (see 9.9.1.3). The value of zero in this field means that there is no Awake Window backoff. See 11.2.1.13.

The Awake Window Duration field is set to the maximum duration of the Awake Window, in units of microseconds. The value zero in this field means that there is no fixed maximum time limit on the Awake Window. See 11.2.1.13.

The Idle Count field is set to the number of consecutive Awake Windows during which no directed frame is received from the TDLS peer STA before a TDLS peer STA deletes the wakeup schedule. See 11.2.1.13.

7.3.2.63 Channel Switch Timing element

The Channel Switch Timing element contains information regarding the channel switch timing. The element is defined in Figure 7-95o30.

	Element ID	Length	Switch Time	Switch Timeout
Octets:	1	1	2	2

Figure 7-95o30—Channel Switch Timing element format

The Length field is set to 4.

The Switch Time field is set to the time it takes for a STA sending the Channel Switch Timing element to switch channels, in units of microseconds.

The Switch Timeout field is set to the maximum time in units of microseconds the STA sending the Channel Switch Timing element will wait for the first data frame exchange on the off-channel before switching back to base channel. The time is measured from the end of the last symbol of the ACK frame that is transmitted in response to TDLS Channel Switch Response frame, as seen at the air interface.

7.3.2.64 PTI Control element

The PTI Control element contains information regarding the traffic buffered at the PU buffer STA for the PU sleep STA at the time a TDLS Peer Traffic Indication frame is transmitted by the PU buffer STA. The element is optionally included in the TDLS Peer Traffic Indication frame. The element is defined in Figure 7-95o31.

	Element ID	Length	TID	Sequence Control
Octets:	1	1	1	2

Figure 7-95o31—PTI Control element format

The Element ID field is defined in Table 7-26.

The Length field is set to 3.

The TID field is set to the highest TID for which the PU buffer STA has traffic buffered that is destined to the PU sleep STA to which the TID field will be transmitted. See 11.2.1.14.

The Sequence Control field is defined in 7.1.3.4. The Sequence Control field contained in the PTI Control element is set to the sequence number of the latest MPDU that has been transmitted over the TDLS direct link to the PU sleep STA that is the destination of the TDLS Peer Traffic Indication frame that contains the PTI Control element. The TID field contained in the PTI Control element is set to the TID of that MPDU. See 11.2.1.14.

7.3.2.65 PU Buffer Status element

The PU Buffer Status element contains information regarding the traffic buffered at the PU buffer STA for the PU sleep STA at the time a TDLS Peer Traffic Indication frame is transmitted by the PU buffer STA. The element is included in the TDLS Peer Traffic Indication frame. The element is defined in Figure 7-95o32.

			B0	B1	B2	B3	B4-B7
	Element ID	Length	AC_BK traffic available	AC_BE traffic available	AC_VI traffic available	AC_VO traffic available	Reserved
Octets:	1	1			1		

Figure 7-95o32—PU Buffer Status element format

The Element ID field is defined in Table 7-26.

The Length field is set to 1.

The AC_BK traffic available field is one bit in size and is set to 1 if AC_BK contains traffic buffered for the PU sleep STA to which the PU Buffer Status element will be transmitted, and is set to 0 otherwise.

The AC_BE traffic available field is one bit in size and is set to 1 if AC_BE contains traffic buffered for the PU sleep STA to which the PU Buffer Status element will be transmitted, and is set to 0 otherwise.

The AC_VI traffic available field is one bit in size and is set to 1 if AC_VI contains traffic buffered for the PU sleep STA to which the PU Buffer Status element will be transmitted, and is set to 0 otherwise.

The AC_VO traffic available field is one bit in size and is set to 1 if AC_VO contains traffic buffered for the PU sleep STA to which the PU Buffer Status element will be transmitted, and is set to 0 otherwise.

7.4 Action frame format details

Insert a new subclause 7.4.11 after subclause 7.4.10:

7.4.11 TDLS Action frame details

Several Action frame formats are defined to support tunneled direct link setup (TDLS). The Action field values associated with each frame format within the TDLS category are defined in Table 7-57v1.

Table 7-57v1—TDLS Action field values

Action field value	Meaning
0	TDLS Setup Request
1	TDLS Setup Response
2	TDLS Setup Confirm
3	TDLS Teardown
4	TDLS Peer Traffic Indication
5	TDLS Channel Switch Request
6	TDLS Channel Switch Response
7	TDLS Peer PSM Request
8	TDLS Peer PSM Response
9	TDLS Peer Traffic Response
10	TDLS Discovery Request
11	TDLS Discovery Response
12 – 255	Reserved

7.4.11.1 TDLS Setup Request frame format

The frame body of a TDLS Setup Request frame contains the information shown in Table 7-57v2.

Table 7-57v2—Information for TDLS Setup Request frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 0, representing TDLS Setup Request.
3	Dialog Token	The Dialog Token field contains a unique non-zero value for the conversation between the STAs involved in this request. The Dialog Token is specified in 7.3.1.12.
4	Link Identifier	The Link Identifier is specified in 7.3.2.61.
5	Capability	The Capability field indicates the capabilities of the STA. The Capability element is defined in 7.3.1.4.
6	Supported rates	The Supported Rates element indicates the rates which are supported by the STA. The Supported Rates element is defined in 7.3.2.2.
7	Extended supported rates	The Extended Supported Rates element is present whenever there are more than eight supported rates, and it is optional otherwise. The Extended Supported Rates element is defined in 7.3.2.14.
8	QoS Capability	The QoS Capability element is present when dot11QosOptionImplemented is true. The QoS Capability element is defined in 7.3.2.35.
9	HT Capabilities	The HT Capabilities element is present when the dot11HighThroughputOptionImplemented attribute is true. The HT Capabilities element is defined in 7.3.2.56.
10	20/40 BSS Coexistence	The 20/40 BSS Coexistence element may appear in this frame. The 20/40 BSS Coexistence element is defined in 7.3.2.60.
11	Extended Capabilities	The Extended Capabilities element may be present if any of the fields in this element are non-zero. The Extended Capabilities element is defined in 7.3.2.27.
12	RSNIE	RSNIE of the TDLS initiator STA (optional). The RSNIE is included if security is required on the direct link. The RSNIE is defined in 7.3.2.25.
13	FTIE	FTIE of the TDLS Initiator (optional). The FTIE is included if security is required on the direct link. The FTIE is defined in 7.3.2.48.
14	Timeout Interval	The Timeout Interval element contains the TPK Key Lifetime (optional). Included if security is required on the direct link. The Timeout Interval element is defined in 7.3.2.49.
15	Supported Channels	The Supported Channels element is defined in 7.3.2.19 (optional). Included if the TDLS channel switching capability field is set to one.
16	Supported Regulatory Classes	The Supported Regulatory Classes element is defined in 7.3.2.51 (optional). Included if the TDLS channel switching capability field is set to one.

17	Country	The Country information element shall be present when dot11MultiDomainCapabilityEnabled is true or dot11SpectrumManagementRequired is true.

The TDLS Setup Request frame is encapsulated in a Data frame and transmitted to the recipient STA through the AP, to request the setup of a TDLS direct link. See 11.19.

7.4.11.2 TDLS Setup Response frame format

The frame body of a TDLS Setup Response frame contains the information shown in Table 7-57v3.

1

Table 7-57v3—Information for TDLS Setup Response frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 1, representing TDLS Setup Response.
3	Status Code	The Status Code is defined in 7.3.1.9.
4	Dialog Token	The Dialog Token is copied from the corresponding TDLS Setup Request. The Dialog Token is specified in 7.3.1.12.
5	Link Identifier	The Link Identifier is specified in 7.3.2.61. Only present for Status Code 0 (Successful).
6	Capability	The Capability field indicates the capabilities of the STA. The Capability element is defined in 7.3.1.4. Included for Status Code 0 (Successful).
7	Supported rates	The Supported Rates element indicates the rates which are supported by the STA. The Supported Rates element is defined in 7.3.2.2. Included for Status Code 0 (Successful).
8	Extended supported rates	The Extended Supported Rates element is present whenever there are more than eight supported rates, and it is optional otherwise. Included for Status Code 0 (Successful). The Extended Supported Rates element is defined in 7.3.2.14.
9	QoS Capability	The QoS Capability element is present when dot11QosOptionImplemented is true and if the Status Code is 0 (Successful). The QoS Capability element is defined in 7.3.2.35.
10	HT Capabilities	The HT Capabilities element is present when the dot11HighThroughputOptionImplemented attribute is true and if the Status Code is 0 (Successful). The HT Capabilities element is defined in 7.3.2.56.
11	20/40 BSS Coexistence	The 20/40 BSS Coexistence element may appear in this frame. Included for Status Code 0 (Successful). The 20/40 BSS Coexistence element is defined in 7.3.2.60.
12	Extended Capabilities	The Extended Capabilities element may be present if any of the fields in this element are non-zero. Included for Status Code 0 (Successful). The Extended Capabilities element is defined in 7.3.2.27.
13	RSNIE	RSNIE of the TDLS responder STA (optional). The RSNIE is included if security is required on the direct link and the Status Code is 0 (Successful). The RSNIE is defined in 7.3.2.25.
14	FTIE	FTIE of the TDLS responder STA (optional). The FTIE is included if security is required on the TDLS direct link and the Status Code is 0 (Successful). The FTIE is defined in 7.3.2.48.
15	Timeout Interval IE	TPK Key Lifetime (optional) Included if security is required on the direct link. Included for Status Code 0 (Successful). The Timeout Interval element is defined in 7.3.2.49.

16	Supported Channels	The Supported Channels element is defined in 7.3.2.19. Included if the TDLS channel switching capability bit is set to one. Included for Status Code 0 (Successful).
17	Supported Regulatory Classes	The Supported Regulatory Classes element is defined in 7.3.2.54. Included if the TDLS channel switching capability bit is set to one . Included for Status Code 0 (Successful).
18	Country	The Country information element shall be present when dot11MultiDomainCapabilityEnabled is true or dot11SpectrumManagementRequired is true.

The TDLS Setup Response frame is encapsulated in a Data frame and transmitted to the TDLS initiator STA through the AP, in response to a received TDLS Setup Request frame. See 11.19.

7.4.11.3 TDLS Setup Confirm frame format

The frame body of a TDLS Setup Confirm frame contains the information shown in Table 7-57v4.

Table 7-57v4—Information for TDLS Setup Confirm frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 2, representing TDLS Setup Confirm.
3	Status Code	The Status Code is defined in 7.3.1.9.
4	Dialog Token	The Dialog Token is copied from the corresponding TDLS Setup Response. The Dialog Token is specified in 7.3.1.12.
5	Link Identifier	The Link Identifier is specified in 7.3.2.61.
6	EDCA Parameter Set	The EDCA parameter set is included when QoS is supported on the direct link. The EDCA Parameter Set element is specified in 7.3.2.29. Included for Status Code 0 (Successful).
7	HT Operation	The HT Operation element is included when dot11HighThroughputOptionImplemented attribute is true and the TDLS Setup Response frame contained an HT Capabilities element (optional). Included for Status Code 0 (Successful). The HT Operation element is defined in 7.3.2.57.
8	FTIE	FTIE of the TDLS initiator STA (optional). The FTIE is included if security is required on the direct link and the Status Code is 0 (Successful). The FTIE is defined in 7.3.2.48.
9	RSNIE	RSNIE (optional). Included if security is required on the direct link. Included for Status Code 0 (Successful). The RSNIE is defined in 7.3.2.25.
10	Timeout Interval IE	TPK Key Lifetime (optional) Included if security is required on the direct link. Included for Status Code 0 (Successful). The Timeout Interval element is defined in 7.3.2.49.

The TDLS Setup Confirm frame is encapsulated in a Data frame and transmitted to the TDLS responder STA through the AP, in response to a received TDLS Setup Response frame. See 11.19.

7.4.11.4 TDLS Teardown frame format

The frame body of a TDLS Teardown frame contains the information shown in Table 7-57v5.

Table 7-57v5—Information for TDLS Teardown frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 3, representing TDLS Teardown.
3	Reason Code	The Reason Code is defined in 7.3.1.7.
4	Link Identifier	The Link Identifier is specified in 7.3.2.61.
5	FTIE	Included if TPK handshake was successful for this session (optional). The FTIE is defined in 7.3.2.48.

The TDLS Teardown frame is encapsulated in a Data frame and transmitted to the TDLS peer STA directly or through the AP, to tear down a TDLS direct link. See 11.19.

7.4.11.5 TDLS Peer Traffic Indication frame format

The frame body of a TDLS Peer Traffic Indication frame contains the information shown in Table 7-57v6.

Table 7-57v6—Information for TDLS Peer Traffic Indication frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24
2	Action	The Action field is set to 4, representing TDLS Peer Traffic Indication.
3	Dialog Token	The Dialog Token is specified in 7.3.1.12.
4	Link Identifier	The Link Identifier is specified in 7.3.2.61.
5	PU Buffer Status	The PU Buffer Status element is defined in 7.3.2.65.
6	PTI Control	The PTI Control element is defined in 7.3.2.64. Optional.

The TDLS Peer Traffic Indication frame indicates the state of the power save buffer at the STA supporting Peer U-APSD that is buffering data for a TDLS peer STA in power save mode.

The Dialog Token field is set to a nonzero value chosen by the STA sending the TDLS Peer Traffic Indication frame to identify the indication/response transaction, when no PTI Control element is included in the TDLS Peer Traffic Indication frame. When a PTI Control element is included in the TDLS Peer Traffic Indication frame, the Dialog Token field is set to zero.

The PU Buffer Status element indicates the status of the AC buffers at the PU buffer STA.

The PTI Control element is optionally included in the TDLS Peer Traffic Indication frame (see 11.2.1.14), to identify the latest MPDU transmitted to the PU sleep STA that is the destination of the TDLS Peer Traffic Indication frame.

The TDLS Peer Traffic Indication frame is encapsulated in a Data frame and transmitted to the TDLS peer STA through the AP. See 11.19.

7.4.11.6 TDLS Channel Switch Request frame format

The frame body of the TDLS Channel Switch Request frame contains the information shown in Table 7-57v7.

Table 7-57v7—Information for TDLS Channel Switch Request frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 5, representing TDLS Channel Switch Request.
3	Target Channel	1 octet field that specifies the channel number of the target channel.
4	Regulatory Class	1 octet field that specifies the regulatory class for the target channel. See 7.3.2.9.
5	Link Identifier	The Link Identifier is specified in 7.3.2.61.
6	Secondary Channel Offset	The secondary channel offset is included only when a switch to a 40 MHz direct link is indicated (optional). See 7.3.2.20a.
7	Channel Switch Timing	The Channel Switch Timing element is specified in 7.3.2.63.

The TDLS Channel Switch Request frame is encapsulated in a Data frame and transmitted directly to the TDLS peer STA, to request for the TDLS direct link to be switched to another channel. See 11.19.

7.4.11.7 TDLS Channel Switch Response frame format

The frame body of the TDLS Channel Switch Response frame contains the information shown in Table 7-57v8.

Table 7-57v8—Information for TDLS Channel Switch Response frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 6, representing TDLS Channel Switch Response.
3	Status Code	The Status Code is defined in 7.3.1.9.
5	Link Identifier	The Link Identifier is specified in 7.3.2.61.
5	Channel Switch Timing	The Channel Switch Timing element is specified in 7.3.2.63

The TDLS Channel Switch Response frame is encapsulated in a Data frame and transmitted directly to the TDLS peer STA, in response to a received TDLS Channel Switch Request frame. See 11.19.

7.4.11.8 TDLS Peer PSM Request frame format

The TDLS Peer PSM Request frame contains the information shown in Table 7-57v9.

Table 7-57v9—Information for TDLS Peer PSM Request frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 7, representing TDLS Peer PSM Request.
3	Dialog Token	The Dialog Token contains a value that is unique among TDLS Peer PSM Request frames for which a corresponding TDLS Peer PSM Response frame has not been received. The Dialog Token is specified in 7.3.1.12.
4	Link Identifier	The Link Identifier is specified in 7.3.2.61.
5	Wakeup Schedule	The Wakeup Schedule is specified in 7.3.2.62.

The TDLS Peer PSM Request frame is encapsulated in a Data frame and transmitted to the TDLS peer STA directly or through the AP, to setup or change a periodic wakeup schedule on the TDLS direct link. See 11.19.

7.4.11.9 TDLS Peer PSM Response frame format

The TDLS Peer PSM Response frame contains the information shown in Table 7-57v10.

Table 7-57v10—Information for TDLS Peer PSM Response frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 8, representing TDLS Peer PSM Response.
3	Dialog Token	The Dialog Token is set to the value contained in the corresponding TDLS Peer PSM Request frame. The Dialog Token is specified in 7.3.1.12.
4	Status Code	The Status Code is specified in 7.3.1.9.
5	Link Identifier	The Link Identifier is specified in 7.3.2.61.
6	Wakeup Schedule	The Wakeup Schedule is only present when the status code is set to 2 ("TDLS Wakeup Schedule rejected but alternative schedule provided"). The Wakeup Schedule is specified in 7.3.2.62.

The TDLS Peer PSM Response frame is encapsulated in a Data frame and transmitted to the TDLS peer STA directly or through the AP, in response to a TDLS Peer PSM Request frame. See 11.19.

7.4.11.10 TDLS Peer Traffic Response frame format

The frame body of a TDLS Peer Traffic Response frame contains the information shown in Table 7-57v11.

Table 7-57v11—Information for TDLS Peer Traffic Response frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24
2	Action	The Action field is set to 9, representing TDLS Peer Traffic Response.
3	Dialog Token	The Dialog Token is specified in 7.3.1.12.
4	Link Identifier	The Link Identifier is specified in 7.3.2.61.

The TDLS Peer Traffic Response frame indicates the receipt of the corresponding TDLS Peer Traffic Indication frame.

The Dialog Token field is set to the nonzero value of the corresponding TDLS Peer Traffic Indication frame.

The Link Identifier field is set to identify the TDLS direct link in relation to which the TDLS Peer Traffic Response frame is transmitted.

The Peer Traffic Response frame is encapsulated in a Data frame and transmitted to the TDLS peer STA directly. See 11.2.1.14.

7.4.11.11 TDLS Discovery Request frame format

The TDLS Discovery Request frame contains the information shown in Table 7-57v12.

1

Table 7-57v12—Information for TDLS Discovery Request frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 10, representing TDLS Discovery Request.
3	Dialog Token	The Dialog Token can be used to match TDLS Discovery Response frames to the corresponding TDLS Discovery Request frame. The Dialog Token is specified in 7.3.1.12.
4	Link Identifier	The Link Identifier element is specified in 7.3.2.65a.
5	Capability	The Capability field indicates the capabilities of the STA. The Capability element is defined in 7.3.1.4.
6	Supported rates	The Supported Rates element indicates the rates which are supported by the STA. The Supported Rates element is defined in 7.3.2.2.
7	Extended supported rates	The Extended Supported Rates element is present whenever there are more than eight supported rates, and it is optional otherwise. The Extended Supported Rates element is defined in 7.3.2.14.
8	HT Capabilities	The HT Capabilities element is present when the dot11HighThroughputOptionImplemented attribute is true. The HT Capabilities element is defined in 7.3.2.56.
9	20/40 BSS Coexistence	The 20/40 BSS Coexistence element is present when the dot112040BSSCoexistenceManagementSupport is true.
10	Extended Capabilities	The Extended Capabilities element may be present if any of the fields in this element are nonzero.
11	RSNIE	The RSNIE may be included if security is required on the direct link. The RSNIE is defined in 7.3.2.25.
12	FTIE	The FTIE may be included if security is required on the direct link. The FTIE is defined in 7.3.2.48.
13	Timeout Interval	The Timeout Interval element contains the TPK Key Lifetime (optional). Included if security is required on the direct link. The Timeout Interval element is defined in 7.3.2.49.
14	Supported Channels	The Supported Channels element is defined in 7.3.2.19 (optional). Included if the TDLS channel switching capability field is set to one.
15	Supported Regulatory Classes	The Supported Regulatory Classes element is defined in 7.3.2.51 (optional). Included if the TDLS channel switching capability field is set to one.
16	TDLS Discovery	Optional. The TDLS Discovery element is specified in 7.3.2.65b.

2

The TDLS Discovery Request frame is encapsulated in a Data frame and transmitted to a TDLS peer STA or to the Broadcast address through the AP, to request TDLS capable STAs in the same BSS to respond with a TDLS Discovery Response frame. See 11.19.

7.4.11.12 TDLS Discovery Response frame format

The TDLS Discovery Response frame contains the information shown in Table 7-57v13.

Table 7-57v13—Information for TDLS Discovery Response frame

Order	Information	Notes
1	Category	The Category field is set to the value for TDLS, as defined in Table 7-24.
2	Action	The Action field is set to 11, representing TDLS Discovery Response.
3	Dialog Token	The Dialog Token is copied from the corresponding TDLS Discovery Request frame. The Dialog Token is specified in 7.3.1.12.
4	Link Identifier	The Link Identifier element is specified in 7.3.2.65a.
5	Capability	The Capability field indicates the capabilities of the STA. The Capability element is defined in 7.3.1.4.
6	Supported rates	The Supported Rates element indicates the rates which are supported by the STA. The Supported Rates element is defined in 7.3.2.2.
7	Extended supported rates	The Extended Supported Rates element is present whenever there are more than eight supported rates, and it is optional otherwise. The Extended Supported Rates element is defined in 7.3.2.14.
8	HT Capabilities	The HT Capabilities element is present when the dot11HighThroughputOptionImplemented attribute is true. The HT Capabilities element is defined in 7.3.2.56.
9	20/40 BSS Coexistence	The 20/40 BSS Coexistence element is present when the dot112040BSSCoexistenceManagementSupport is true.
10	Extended Capabilities	The Extended Capabilities element may be present if any of the fields in this element are nonzero.
11	RSNIE	The RSNIE may be included if security is required on the direct link. The RSNIE is defined in 7.3.2.25.
12	FTIE	The FTIE may be included if security is required on the direct link. The FTIE is defined in 7.3.2.48.
13	Timeout Interval	The Timeout Interval element contains the TPK Key Lifetime (optional). Included if security is required on the direct link. The Timeout Interval element is defined in 7.3.2.49.
14	Supported Channels	The Supported Channels element is defined in 7.3.2.19 (optional). Included if the TDLS channel switching capability field is set to one.
15	Supported Regulatory Classes	The Supported Regulatory Classes element is defined in 7.3.2.51 (optional). Included if the TDLS channel switching capability field is set to one.
16	TDLS Discovery	Optional. The TDLS Discovery element is specified in 7.3.2.65b.

The TDLS Discovery Response frame is encapsulated in a Data frame and transmitted directly (i.e., not via the AP) to the TDLS peer STA that sent the corresponding TDLS Discovery Request frame. See 11.19.

8. Security

8.4 RSNA security association management

8.4.1 Security associations

8.4.1.1 Security association definitions

Insert a new subclause 8.4.1.1.6 after 8.4.1.1.5

8.4.1.1.6 TPKSA

The TPKSA results from a successful completion of the TDLS Peer Key Handshake. This security association is bidirectional between the TDLS initiator STA and the TDLS responder STA. The TPKSA is used to create session keys to protect this TDLS session. The TPKSA is cached per the lifetime indicated in the TDLS Peer Key Handshake or until the TDLS direct link is torn down, whichever comes first.

The TPKSA consist of the following:

- MAC addresses of the TDLS initiator STA and the TDLS responder STA
- Pairwise cipher suite selector
- TPK Lifetime
- TPK Name
- TPK
- Link Identifier

8.5 Keys and key distribution

Insert a new subclause 8.5.9 after subclause 8.5.8 as follows:

8.5.9 TDLS Peer Key Security Protocol

The TDLS Peer Key security protocol is executed between the two non-AP STAs that intend to establish an RSNA for direct link communication. The TDLS Peer Key security protocol shall not be used when either STA has a connection with the AP that is protected using WEP, because WEP may cause the key material to get leaked.

8.5.9.1 TDLS Peer Key Handshake

The TDLS Peer Key (TPK) handshake occurs as part of the TDLS Direct Link setup procedure. The TPKSA is the result of the successful completion of the TDLS Peer Key Handshake protocol, which derives keys for providing confidentiality and data origin authentication.

In order to maintain TPK confidentiality, both the TDLS initiator STA and the TDLS responder STAs must establish an RSNA with their common AP prior to executing the TDLS Peer Key handshake. To meet this criteria, a STA shall not initiate the TDLS Peer Key Handshake and shall reject any TDLS setup messages requesting to construct a TPKSA if

1. The AP does not include an RSNIE in its Beacons and Probe Responses to advertise the availability of security;
2. The AP's RSN IE indicates that WEP-40 (OUI 00-0F-AC:1) or WEP-104 (OUI 00-0F-AC:5) are enabled as either pairwise or group cipher suites; or
3. The AP's RSN IE indicates that Use group cipher suite (00-0F-AC:0) is used as the pairwise cipher suite.

Violation of any of these cases would cause the TDLS Peer Key handshake to leak the TPK.

The TDLS initiator STA and the TDLS responder STA perform the following exchange to setup a TPK.

TDLS PMK Handshake Message 1: TDLS initiator STA → TDLS responder STA
Link Identifier IE, RSNIE, Timeout Interval IE, FTIE

TDLS PMK Handshake Message 2: TDLS responder STA -> TDLS initiator STA
Link Identifier IE, RSNIE, Timeout Interval IE, FTIE

TDLS PMK Handshake Message 3: TDLS initiator STA -> TDLS responder STA
Link Identifier IE, RSNIE, Timeout Interval IE, FTIE

where

- The TDLS initiator STA Address field of the Link Identifier element is the MAC address of the TDLS initiator STA;
- The TDLS responder STA Address field of the Link Identifier element is the MAC address of the TDLS responder STA;
- The PairwiseCipherSuite field of the RSNIE identifies the cipher suite used to protect the data frames sent over the direct link;
- The AKM suite list of the RSNIE identifies which Authentication Method was used;
- The TimeoutIntervalType field of the Timeout Interval IE is the key lifetime;
- The SNonce field of the FTIE is a 256 bit value randomly generated by the TDLS initiator STA;
- The ANonce field of the FTIE is a 256 bit value randomly generated by the TDLS responder STA (set to 0 in message 1);
- The MIC field of the FTIE is zero for message 1 and computed as described in 8.9.5.3.3 and 8.9.5.3.4 for messages 2 and 3 respectively;

The TDLS PMK Handshake Message 1 shall be transmitted in the TDLS Setup Request frame.

TDLS PMK Handshake Message 2 shall be transmitted in the TDLS Setup Response frame.

TDLS PMK Handshake Message 3 shall be transmitted in the TDLS Setup Confirm frame.

The TPK shall be derived as follows:

TPK-Key-Input = SHA-256(min (SNonce, ANonce) || max (SNonce, ANonce))

TPK-Key-Data = KDF-N_KEY(TPK-Key-Input, "TDLS PMK", min (MAC_I, MAC_R)
|| max (MAC_I, MAC_R) || BSSID || N_KEY)

TPK = L(TPK-Key-Data, 0, TK_bits)

where

- N_KEY = TK_bits + 128. TK_bits is cipher-suite specific and specified in table 8.2
- KDF-N_KEY is the key derivation function defined in 8.5.1.5.2.

The TPK-Name shall be derived as follows:

TPK-Name-Salt = L(TPK-Key-Data, TK_bits, 128)

TPK-Name = Truncate-128(SHA-256("TDLS PMK Name" || TPK-Name-Salt))

MAC_I and MAC_R are the MAC addresses of the TDLS initiator STA and the TDLS responder STA, respectively. SNonce and ANonce are the nonces generated by the TDLS initiator STA and TDLS responder STA, respectively, for this instance of the TPK handshake. The BSSID is set to the BSSID of the current association of the TDLS initiator STA.

Each TPK has two component keys, TPK-KCK, and TPK-TK, defined as follows:

The Key Confirmation Key (KCK) shall be computed as the first 128 bits (bits 0-127) of the TPK

TPK-KCK = L(TPK, 0, 128)

where, L(-) is defined in 8.5.1.

The KCK is used to provide data origin authenticity in TDLS Setup Response and TDLS Setup Confirm messages.

The Temporal keys (TK) shall be computed as the remaining bits (for CCMP, the second 128 bits, i.e., bits 128-255) of the TPK

TPK-TK = L(TPK, 128, N_KEY – 128)

The TPK-TK is used to provide confidentiality for direct link data and management messages.

The temporal key is configured into the STA by the SME through the use of the MLME-SETKEYS.request primitive.

8.5.9.2 TDLS Peer Key Handshake Security Assumptions

The security of the TDLS PMK handshake depends on:

a. The TDLS initiator STA and the TDLS peer STA each have an RSNA established with the AP that is being used for TDLS Setup.
b. The AP does not expose the nonces exchanged by the TDLS initiator STA and the TDLS responder STA to any external party.
c. The AP does not use these nonces to derive the TPK and attack the TDLS direct link instance.
d. TDLS message security (encryption and integrity computations) processing at the AP is protected from illegal eavesdropping, alterations, insertions and substitutions.
e. The TDLS initiator STA and TDLS responder STAs do not expose SNonce, ANonce, or the derived key to a third party.
f. The TDLS initiator STA and the TDLS peer STA are associated to the same AP.

8.5.9.3 TDLS Peer Key (TPK) Security Protocol Handshake Messages

8.5.9.3.1. Overview

The TDLS Peer Key Handshake consists of three messages. Each message is comprised of a number of information elements, and is included in the TDLS Setup Request, TDLS Setup Response, and TDLS Setup Confirm.

In an RSN, these handshake messages serve to provide a session identifier, are identified by the nonces, and are used as association instance identifiers. These nonces are chosen randomly or pseudo randomly, and are used to generate the TPK.

8.5.9.3.2 TPK Handshake Message 1

If the TDLS initiator STA has an RSNA with the BSS, it shall add an RSN IE, FTIE, and Timeout Interval IE to its TDLS Setup Request frame. The IEs shall be formatted as follows:

- The RSN information element, if present, shall be set as follows:
  - Version shall be set to 1.
  - The pairwise cipher suite list field indicating the pairwise cipher suites the TDLS initiator STA is willing to use with the TPKSA. WEP-40 and WEP-104 shall not be included in this list. The pairwise cipher suite list field shall only include pairwise cipher suites that are advertised in the RSNIE of the BSS.
  - The group cipher suite shall be set to 00-00-00:0.
  - The AKM suite count field shall be set to 1.
  - The AKM suite list field shall be set to TPK Handshake (00-0F-AC:7).
  - The Capabilities field shall set the 'No Pairwise' subfield to 0 and 'Peer Key Enabled' subfield to 1.
  - PMKID count shall be 0.
  - PMKID list shall not be present.

- Include the lifetime of the TPKSA in the Timeout Interval IE using Lifetime Interval Type as '2' (Key Lifetime Interval). The minimum lifetime shall be 300 seconds.

- The Fast BSS Transition information element (FTIE) shall be present only if dot11RSNAEnabled is true. If present, the FTIE shall be set as follows:
  - SNonce shall be set to a value chosen randomly by the TDLS initiator STA, following the recommendations of 8.5.7.
  - All other fields shall be set to 0.

The TDLS initiator STA sends Message 1 to the TDLS responder STA.

On reception of Message 1, the TDLS responder STA checks whether the RSNIE is present.

- If the TDLS responder STA does not have an RSNA with the AP, it shall reject the request with status code 5 ("Security disabled").

- If the TDLS responder STA does have an RSNA with the AP, it checks whether the request includes an RSN IE. If not, the TDLS responder STA shall reject the request with status code 38 ("The request has not been successful as one or more parameters have invalid values").

- If the version field of the RSN IE is zero, then the TDLS responder STA shall reject the request with status code 44 ("Unsupported RSN information element version").

- Otherwise, the TDLS responder STA checks the version field of the RSN IE. When the RSN IE version is greater than or equal to 1 the TDLS responder STA processes the message as follows:

  – If the contents of the RSNIE do not indicate AKM of TPK Handshake (suite type 00-0F-AC:7), the TDLS responder STA shall reject the request with status code 43 ("Invalid AKMP").

  – If any pairwise cipher suite included in the pairwise cipher suite list field of the RSNIE is not advertised in the RSNIE of the BSS, the TDLS responder STA shall reject the request with status code 42 (“Invalid pairwise cipher”).

  – If none of the pairwise cipher suites are acceptable, or Pairwise ciphers include WEP-40 or WEP-104, then the TDLS responder STA shall reject the TDLS Setup Request with status code 42 (“Invalid pairwise cipher”).

  – If the RSN Capabilities field has not set the subfields according to the described rules for this message, then the TDLS responder STA rejects with status code 45 (“Invalid RSN information element capabilities”).

  – If the suggested lifetime is unacceptable or below the default value, the TDLS responder STA shall reject the TDLS Setup Request with status code 6 (“Unacceptable lifetime”)

  – If the contents of the FTIE are not as per specified for this message, then the TDLS responder STA shall reject the TDLS Setup Request with status code 55 (“Invalid FTIE”).

  – The TDLS responder STA shall ignore the remaining fields in the RSNIE FTIE and Timeout Interval IE.

  – Otherwise, the TDLS responder STA shall respond as specified in 11.19.2.

8.5.9.3.3 TPK Handshake Message 2

If the TDLS responder STA validates the TPK Handshake Message 1 for this TDLS instance, the TDLS responder STA may respond with TPK Handshake Message 2. To do so, the TDLS responder STA shall add an RSN IE, FTIE, and Timeout Interval IE to its TDLS Setup Response frame. The IEs shall be formatted as follows:

- The RSN IE shall include the following:
  - Include a pairwise cipher suite from one of those presented in RSN IE of message 1 of this sequence in the Pairwise Cipher Suite List, and set the Pairwise Cipher Suite count to 1.
  - The version number shall be the minimum of the maximum version supported by the TDLS responder STA and the version number received in the RSNIE of Message 1.
  – All other RSN IE fields shall be same as those received in Message 1.

- The Timeout Interval IE shall be the same as that received in the TPK Handshake message 1.

- The FTIE shall include the following:
  – ANonce shall be set to a value chosen randomly by the TDLS responder STA, following the recommendations of 8.5.7.
  – SNonce shall be same as that received in message 1 of this sequence

- The MIC shall be calculated on the concatenation, in the following order, of:
  - TDLS initiator STA MAC address (6 octets)
  - TDLS responder STA MAC address (6 octets)
  - Transaction Sequence number (1 octet) which shall be set to the value 2
  - Link Identifier IE
  - RSN IE
  - Timeout Interval IE
  - FTIE, with the MIC field of the FTIE set to 0.

  The MIC shall be calculated using the TPK-KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
- All other fields shall be set to 0.

The TDLS responder STA sends Message 2 to the TDLS initiator STA. The TDLS initiator STA shall process Message 2 as follows:

- If the TDLS initiator STA Address and TDLS responder STA Address of the Link Identifier element do not match those for an outstanding TDLS Setup Request, the TDLS initiator STA shall reject the response with status code 70 ("Unexpected message").

- If the SNonce field of the FTIE does not match that of an outstanding request to the TDLS responder STA, then the TDLS initiator STA shall reject the response with status code 71 ("Invalid SNonce") .

- Otherwise, the TDLS initiator STA shall compute the TPK and then validate the MIC in the FTIE as specified in MIC calculation procedure for TPK Handshake Message 2. If invalid, the TDLS initiator STA shall discard the message.

- If the version of the RSN IE is zero or is greater than the version of the RSN IE sent in Message 1, then the TDLS initiator STA shall reject the response with status code 44 ("Unsupported RSN information element version). Otherwise, the TDLS initiator STA shall:
  - If the contents of the RSNIE, with the exception of the Pairwise cipher suite count and Pairwise cipher suite list are not the same as those sent by the TDLS initiator STA in Message 1 of this sequence, then the TDLS initiator STA shall reject the response with status code 72 ("Invalid contents of RSNIE");
  - If the Pairwise Cipher Suite count is other than 1, then the TDLS initiator STA shall reject the response with status code 42 ("Invalid pairwise cipher");
  - If the selected pairwise cipher suite was not included in the Initiator's request, then the TDLS initiator STA shall reject the TDLS Setup Response with status code 42 ("Invalid pairwise cipher");
  - If the Timeout Interval IE is not the same as that sent in Message 1, the TDLS initiator STA shall reject the TDLS Setup Response with status code 6 ("Unacceptable lifetime");
  - If the BSSID in the Link Identifier element is different from the one sent in Message 1, then the TDLS initiator STA shall reject the response with status code 7 ("Not in same BSS").

If the TDLS initiator STA validates TDLS Message 2, the TDLS initiator STA shall create a TPKSA and respond with Message 3 as defined in 11.19.2. The TDLS initiator STA uses the MLME-SETKEYS.request primitive to configure the Temporal Key into its STA.

8.5.9.3.4 TPK Handshake Message 3

If the TDLS initiator STA wants to respond to Message 2 for this TDLS instance, the TDLS initiator STA shall add an RSN IE, FTIE, and Timeout Interval IE to its TDLS Setup Confirm frame. The IEs shall be formatted as follows:

- The RSN information element shall be present only if dot11RSNAEnabled is true. If present, the RSNIE shall be the same as the RSNIE received in Message 2.

- The Timeout Interval IE shall be the same as that received in the TPK Handshake message 1.

- The Fast BSS Transition information element (FTIE) shall be present only if dot11RSNAEnabled is true. If present, with the exception of the MIC field, the contents of the FTIE shall be the same as the FTIE received in Message 2.
  - The MIC shall be calculated on the concatenation, in the following order, of:
    - TDLS initiator STA MAC address (6 octets)
    - TDLS responder STA MAC address (6 octets)
    - Transaction Sequence number (1 octet) which shall be set to the value 3
    - Link Identifier IE
    - RSN IE
    - Timeout Interval IE
    - FTIE, with the MIC field of the FTIE set to 0.

    The MIC shall be calculated using the TPK-KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
  - All other fields shall be set to 0.

The TDLS initiator STA sends Message 3 to the TDLS responder STA. The TDLS responder STA shall process Message 3 as follows:

– If the Source and Destination Addresses of the Link Identifier IE do not match those for an outstanding TDLS Setup Request, the TDLS responder STA shall discard the message.
– If the ANonce and SNonce fields of the FTIE do not match that of an outstanding request to the TDLS initiator STA, then the TDLS responder STA shall discard the message.
– Otherwise, the TDLS responder STA shall validate the MIC in the FTIE as specified in the MIC calculation procedure for TPK Handshake Message 3. If invalid, the TDLS responder STA shall discard the message.
– If any of the following checks fail, then the TDLS responder STA shall discard the message, the TDLS responder STA shall abandon the TPK Handshake identified by the <ANonce, SNonce> combination, and delete existing TPK Handshake Key state for this sequence.
  - Contents of RSNIE are not the same as what were sent by the TDLS responder STA in Message 2
  - The Timeout Interval IE is not the same as that sent in Message 2
  - The BSSID from the Link Identifier element is not the same as that sent in Message 2

On successful processing of Message 3, the TPK Handshake is considered successful, and the TDLS peer STA shall use the MLME-SETKEYS.request primitive to configure the Temporal Key into its STA.

10. Layer management

10.3 MLME SAP interface

Insert new subclauses 10.3.44 through 10.3.48 at the end of clause 10.3 as follows:

10.3.44 TDLS Direct Link Establishment

The following MLME primitives support the signaling of tunneled direct link setup. Figure 10-6a depicts the TDLS direct link establishment process. The figure is only an example of the basic procedure and is not meant to be exhaustive of all possible uses of the protocol.

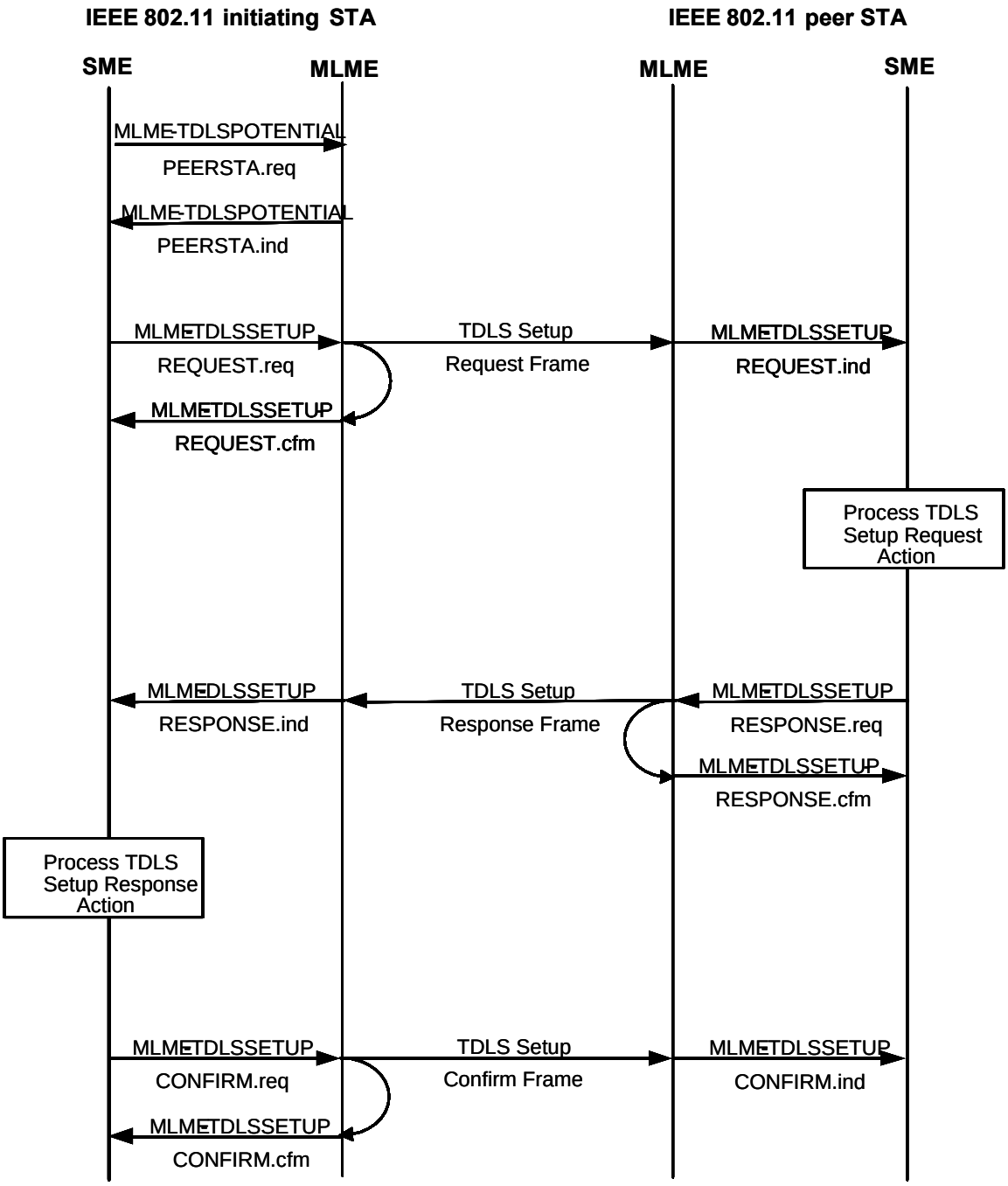

Figure 10-6a—TDLS direct link Establishment

10.3.44.1 MLME-TDLSSETUPREQUEST.request

10.3.44.1.1 Function

This primitive requests that a TDLS Setup Request frame be sent to a candidate TDLS responder STA.

10.3.44.1.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPREQUEST.request(
TDLSResponderAddress,
TDLSSetupRequest,
TDLSResponseTimeout
)

Name	Type	Valid Range	Description
TDLSResponderAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the STA to which the TDLS Setup Request frame must be transmitted.
TDLSSetupRequest	Sequence of octets	As defined in TDLS Setup Request frame	Specifies the proposed service parameters for the TDLS Setup.
TDLSResponseTimeout	Integer	≥ 0	Specifies a time limit (in TU) after which the TDLS Setup procedure is terminated.

10.3.44.1.3 When Generated

This primitive is generated by the SME to request that a TDLS Setup Request frame be sent to a candidate TDLS responder STA.

10.3.44.1.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Setup Request frame. The STA then attempts to transmit this frame to the candidate TDLS responder STA.

10.3.44.2 MLME-TDLSSETUPREQUEST.confirm

10.3.44.2.1 Function

This primitive reports the result of an MLME-TDLSSETUPREQUEST.request primitive to establish a direct link with a candidate TDLS responder STA.

10.3.44.2.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPREQUEST.confirm(
TDLSResponderAddress,
ResultCode
)

Name	Type	Valid Range	Description
TDLSResponderAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the STA to which the TDLS Setup Request frame was attempted to be transmitted.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, TIMEOUT, UNSPECIFIED_FAILURE, NOT_IN_SAME_BSS	Indicates the results of the corresponding MLME-TDLSSETUPREQUEST.request primitive.

10.3.44.2.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSSETUPREQUEST.request and indicates the results of the request.

This primitive is generated when the STA successfully transmits a TDLS Setup Request frame to the AP, when the MLME-TDLSSETUPREQUEST.request contains invalid parameters, when a timeout or an unspecified failure occurs.

10.3.44.2.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSSETUPREQUEST.request primitive and may use the reported data.

10.3.44.3 MLME-TDLSSETUPREQUEST.indication

10.3.44.3.1 Function

This primitive indicates that a TDLS Setup Request frame was received.

10.3.44.3.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPREQUEST.indication(
TDLSInitiatorAddress,
TDLSSetupRequest
)

Name	Type	Valid Range	Description
TDLSInitiatorAddress	MACAddress	Any valid individual MAC Address	Specifies the MAC address of the TDLS initiator STA from which a TDLS Setup Request frame was received.
TDLSSetup Request	Sequence of octets	As defined in TDLS Setup Request frame	Specifies the proposed service parameters for the TDLS Setup.

10.3.44.3.3 When Generated

This primitive is generated by the MLME when a valid TDLS Setup Request frame is received.

10.3.44.3.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure in 11.19.

10.3.44.4 MLME-TDLSSETUPRESPONSE.request

10.3.44.4.1 Function

This primitive requests that a TDLS Setup Response frame be sent to the TDLS initiator STA.

10.3.44.4.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSSETUPRESPONSE.request(
                    TDLSInitiatorAddress,
                    TDLSSetupResponse,
                    TDLSResponseTimeout
                    )
```

Name	Type	Valid Range	Description
TDLSInitiatorAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS initiator STA to which a TDLS Setup Response frame must be transmitted.
TDLSSetupResponse	Sequence of octets	As defined in TDLS Setup Response frame	Specifies the proposed service parameters for the TDLS Setup.
TDLSResponseTimeout	Integer	≥ 0	Specifies a time limit (in TU) after which the TDLS Setup procedure is terminated.

10.3.44.4.3 When Generated

This primitive is generated by the SME to request that a TDLS Setup Response frame be sent to the TDLS initiator STA.

10.3.44.4.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Setup Response frame. The STA then attempts to transmit this to the TDLS initiator STA.

10.3.44.5 MLME-TDLSSETUPRESPONSE.confirm

10.3.44.5.1 Function

This primitive reports the result of an MLME-TDLSSETUPRESPONSE.request primitive to transmit a TDLS Setup Response frame to a TDLS initiator STA.

10.3.44.5.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPRESPONSE.confirm(
TDLSInitiatorAddress,
ResultCode
)

Name	Type	Valid Range	Description
TDLSInitiatorAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS initiator STA to which the TDLS Setup Response frame was attempted to be transmitted.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, TIMEOUT, UNSPECIFIED_FAILURE,	Indicates the results of the corresponding MLME-TDLSSETUPRESPONSE.request primitive.

10.3.44.5.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSSETUPRESPONSE.request and indicates the results of the request.

This primitive is generated when the STA successfully transmits a TDLS Setup Response frame to the AP, when the MLME-TDLSSETUPRESPONSE.request contains invalid parameters, or when a timeout or an unspecified failure occurs.

10.3.44.5.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSSETUPRESPONSE.request primitive and may use the reported data.

10.3.44.6 MLME-TDLSSETUPRESPONSE.indication

10.3.44.6.1 Function

This primitive indicates that a TDLS Setup Response frame was received from the TDLS responder STA.

10.3.44.6.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPRESPONSE.indication(
TDLSResponderAddress,
TDLSSetupResponse
)

Name	Type	Valid Range	Description
TDLSResponder Address	MACAddress	Any valid individual MAC Address	Specifies the MAC address of the TDLS responder STA from which a TDLS Setup Response frame was received.
TDLSSetup Response	Sequence of octets	As defined in TDLS Setup Response frame	Specifies the proposed service parameters for the TDLS Setup.

10.3.44.6.3 When Generated

This primitive is generated by the MLME when a valid TDLS Setup Response frame is received.

10.3.44.6.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure in 11.19.

10.3.44.7 MLME-TDLSSETUPCONFIRM.request

10.3.44.7.1 Function

This primitive requests that a TDLS Setup Confirm frame be sent to the TDLS responder STA.

10.3.44.7.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPCONFIRM.request(
TDLSResponderAddress,
TDLSSetupConfirm,
TDLSResponseTimeout
)

Name	Type	Valid Range	Description
TDLSResponderAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS responder STA to which a TDLS Setup Confirm frame must be transmitted.
TDLSSetupConfirm	Sequence of octets	As defined in TDLS Setup Confirm frame	Specifies the proposed service parameters for the TDLS Setup.
TDLSResponseTimeout	Integer	≥ 0	Specifies a time limit (in TU) after which the TDLS Setup procedure is terminated.

10.3.44.7.3 When Generated

This primitive is generated by the SME to request that a TDLS Setup Confirm frame be sent to the TDLS responder STA.

10.3.44.7.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Setup Confirm frame. The STA then attempts to transmit this to the TDLS responder STA.

10.3.44.8 MLME-TDLSSETUPCONFIRM.confirm

10.3.44.8.1 Function

This primitive reports the result of an MLME-TDLSSETUPCONFIRM.request primitive to transmit a TDLS Setup Response frame to the TDLS responder STA.

10.3.44.8.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSSETUPCONFIRM.confirm(
TDLSResponderAddress,
ResultCode
)

Name	Type	Valid Range	Description
TDLSResponder Address	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS responder STA to which the TDLS Setup Confirm frame was attempted to be transmitted.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, TIMEOUT, UNSPECIFIED_FAILURE,	Indicates the results of the corresponding MLME-TDLSSETUPCONFIRM.request primitive.

10.3.44.8.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSSETUPCONFIRM.request and indicates the results of the request.

This primitive is generated when the STA successfully transmits a TDLS Setup Confirm frame to the AP, when the MLME-TDLSSETUPCONFIRM.request contains invalid parameters, when a timeout or an unspecified failure occurs.

10.3.44.8.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSSETUPCONFIRM.request primitive and may use the reported data.

10.3.44.9 MLME-TDLSSETUPCONFIRM.indication

10.3.44.9.1 Function

This primitive indicates that a TDLS Setup Confirm frame was received from the TDLS initiator STA.

10.3.44.9.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSSETUPCONFIRM.indication(
                    TDLSInitiatorAddress,
                    TDLSSetupConfirm
                    )
```

Name	Type	Valid Range	Description
TDLSInitiatorAddress	MACAddress	Any valid individual MAC Address	Specifies the MAC address of the TDLS initiator STA from which a TDLS Setup Confirm frame was received.
TDLSSetup Confirm	Sequence of octets	As defined in TDLS Setup Confirm frame	Specifies the proposed service parameters for the TDLS Setup.

10.3.44.9.3 When Generated

This primitive is generated by the MLME when a valid TDLS Setup Confirm frame is received.

10.3.44.9.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure in 11.19.

10.3.44.10 MLME-TDLSPOTENTIALTDLSPEERSTA.request

10.3.44.10.1 Function

This primitive requests information about a potential TDLS peer STA.

10.3.44.10.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSPOTENTIALTDLSPEERSTA.request(
                    MACAddress
                    )
```

Name	Type	Valid Range	Description
MACAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the potential TDLS peer STA.

10.3.44.10.3 When Generated

This primitive is generated by the SME to request the MLME to provide information about a potential TDLS peer STA.

10.3.44.10.4 Effect of Receipt

On receipt of this primitive, the MLME responds with the requested information about the identified STA.

10.3.44.11 MLME-TDLSPOTENTIALTDLSPEERSTA.confirm

10.3.44.11.1 Function

This primitive informs the SME about a potential TDLS peer STA.

10.3.44.11.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSPOTENTIALTDLSPEERSTA.confirm(
MACAddress,
RSSI,
VendorSpecificInfo
)

Name	Type	Valid Range	Description
MACAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the STA for which information is requested.
STA RSSI	Integer	-1-RSSI Max	Specifies the RSSI from the STA. -1 indicates that the STA is not present.
VendorSpecificInfo	Vendor Specific	Vendor Specific	Specifies vendor specific information about the STA identified in the MACAddress field.

10.3.44.11.3 When Generated

This primitive is generated by the MLME to indicate to the SME that a potential TDLS peer STA has been detected.

10.3.44.11.4 Effect of Receipt

On receipt of this primitive, the SME may attempt to set up a TDLS direct link by issuing an MLME-TDLSSETUPREQUEST.request primitive to the MLME.

10.3.45 TDLS Direct Link Teardown

The following MLME primitives support the signaling of tunneled direct link setup. Figure 10-6b depicts the TDLS direct link teardown process. The figure is only an example of the basic procedure and is not meant to be exhaustive of all possible uses of the protocol.

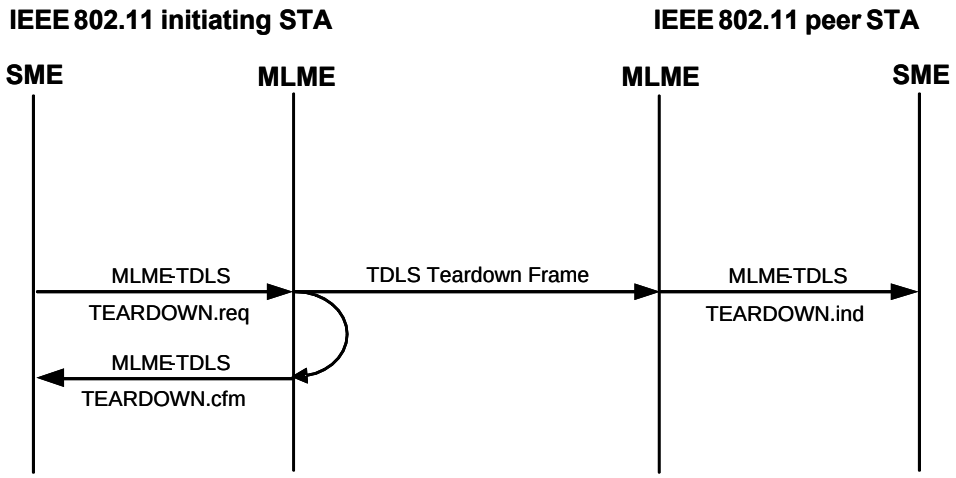

Figure 10-6b—TDLS Direct Link Teardown

10.3.45.1 MLME-TDLSTEARDOWN.request

10.3.45.1.1 Function

This primitive requests that a TDLS Teardown frame be sent to the TDLS peer STA.

10.3.45.1.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSTEARDOWN.request(
TDLSPeerSTAAddress,
TDLSTeardown
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA to which a TDLS Teardown frame must be transmitted.
TDLSTeardown	Sequence of octets	As defined in TDLS Teardown frame	Specifies the proposed service parameters for the TDLS Teardown.

10.3.45.1.3 When Generated

This primitive is generated by the SME to request that a TDLS Teardown frame be sent to the TDLS peer STA.

10.3.45.1.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Teardown frame. The STA then attempts to transmit this frame to the TDLS peer STA.

10.3.45.2 MLME-TDLSTEARDOWN.confirm

10.3.45.2.1 Function

This primitive reports the result of an MLME-TDLSTEARDOWN.request primitive to transmit a TDLS Teardown frame.

10.3.45.2.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSTEARDOWN.confirm(
TDLSPeerSTAAddress,
ResultCode
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of TDLS peer STA to which a TDLS Teardown frame was attempted to be transmitted.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, UNSPECIFIED_FAILURE,	Indicates the results of the corresponding MLME-TDLSTEARDOWN.request primitive.

10.3.45.2.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSTEARDOWN.request and indicates the results of the request.

This primitive is generated when the STA successfully transmits a TDLS Teardown frame to the TDLS peer STA, when the MLME-TDLSTEARDOWN.request contains invalid parameters, or when an unspecified failure occurs.

10.3.45.2.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSTEARDOWN.request primitive and may use the reported data.

10.3.45.3 MLME-TDLSTEARDOWN.indication

10.3.45.3.1 Function

This primitive indicates that a TDLS Teardown frame was received from a TDLS peer STA.

10.3.45.3.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSTEARDOWN.indication(
TDLSPeerSTAAddress,
TDLSTeardown
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MACAddress	Any valid individual MAC Address	The MAC address of the TDLS peer STA from which a TDLS Teardown frame was received.
TDLSTeardown	Sequence of octets	As defined in TDLS Teardown frame	Specifies the proposed service parameters for the TDLS Teardown.

10.3.45.3.3 When Generated

This primitive is generated by the MLME when a valid TDLS Teardown frame is received.

10.3.45.3.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure in 11.19.

10.3.46 TDLS Peer U-APSD

The following MLME primitives support the signaling of Peer U-APSD. Figure 10-6c depicts the TDLS Peer U-APSD process. The figure is only an example of the basic procedure and is not meant to be exhaustive of all possible uses of the protocol.

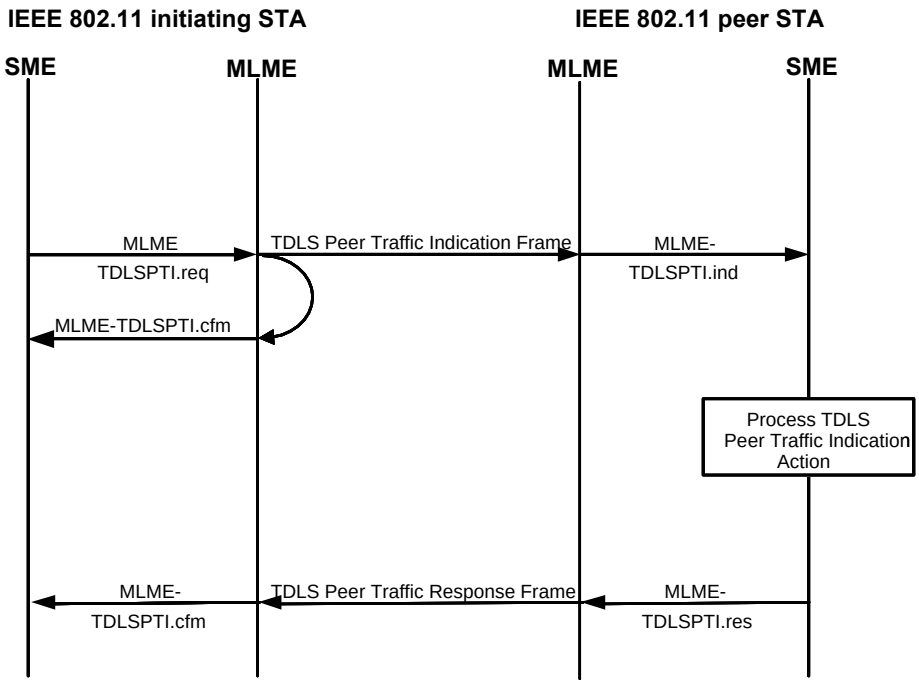

Figure 10-6c—TDLS Peer U-APSD

10.3.46.1 MLME-TDLSPTI.request

10.3.46.1.1 Function

This primitive requests that a TDLS Peer Traffic Indication frame be sent to a TDLS peer STA.

10.3.46.1.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSPTI.request(
                    TDLSPeerSTAAddress,
                    TDLSPTI
                    )
```

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the MAC entity with which to perform the TDLS peer U-APSD process.
TDLSPTI	Sequence of octets	As defined in TDLS Peer Traffic Indication frame	Specifies the proposed service parameters for the TDLS Peer U-APSD.

10.3.46.1.3 When Generated

This primitive is generated by the SME to request that a TDLS Peer Traffic Indication frame be sent to the TDLS peer STA.

10.3.46.1.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Peer Traffic Indication frame. The STA then attempts to transmit this to the TDLS peer STA.

10.3.46.2 MLME-TDLSPTI.confirm

10.3.46.2.1 Function

This primitive reports the result of an MLME-TDLSPTI.request primitive to trigger an unscheduled SP from a candidate TDLS peer STA. This primitive is generated after transmitting a Peer Traffic Indication frame when this frame contains a PTI Control field, and after receiving a Peer Traffic Response frame otherwise.

10.3.46.2.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSPTI.confirm(
                    TDLSPeerSTAAddress,
                    ResultCode,
```

TDLSPTR
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the peer MAC entity with which to perform the TDLS Peer U-APSD process.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, UNSPECIFIED_FAILURE,	Indicates the results of the corresponding MLME-TDLSPTI.request primitive.
TDLSPTR	Sequence of octets	As defined in TDLS Peer Traffic Response frame	If the ResultCode was SUCCESS, specifies the proposed service parameters for the TDLS Peer U-APSD.

10.3.46.2.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSPTI.request and indicates the results of the request.

This primitive is generated when the STA successfully receives a TDLS Peer Traffic Response frame from the TDLS peer STA, when the MLME-TDLSPTI.request contains invalid parameters, or when an unspecified failure occurs.

10.3.46.2.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSPTI.request primitive and may use the reported data.

10.3.46.3 MLME-TDLSPTI.indication

10.3.46.3.1 Function

This primitive indicates that a TDLS Peer Traffic Indication frame was received from a TDLS peer STA.

10.3.46.3.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSPTI.indication(
TDLSPeerSTAAddress,
TDLSPTI
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MACAddress	Any valid individual MAC Address	The MAC address of the non-AP STA MAC entity from which a TDLS Peer Traffic Indication frame was received.
TDLSPTI	Sequence of octets	As defined in TDLS Peer Traffic Indication frame	Specifies the proposed service parameters for the TDLS Peer U-APSD.

10.3.46.3.3 When Generated

This primitive is generated by the MLME when a valid TDLS Peer Traffic Indication frame is received.

10.3.46.3.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure as specified in 11.2.1.14.

10.3.46.4 MLME-TDLSPTI.response

10.3.46.4.1 Function

This primitive requests that a TDLS Peer Traffic Response frame be sent to the TDLS peer STA.

10.3.46.4.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSPTI.response(
PeerSTAAddress,
TDLSPTR
)

Name	Type	Valid Range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the peer MAC entity with which to perform the TDLS Peer U-APSD.
TDLSPTR	Sequence of octets	As defined in TDLS Peer Traffic Response frame	Specifies the proposed service parameters for the TDLS Peer U-APSD.

10.3.46.4.3 When Generated

This primitive is generated by the SME to request that a TDLS Peer Traffic Response frame be sent to the TDLS peer STA.

10.3.46.4.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Peer Traffic Response frame. The STA then attempts to transmit this to the TDLS peer STA.

10.3.47 TDLS Channel Switching

The following MLME primitives support the signaling of a TDLS channel switch. Figure 10-6d depicts the TDLS channel switching process. The figure is only an example of the basic procedure and is not meant to be exhaustive of all possible uses of the protocol.

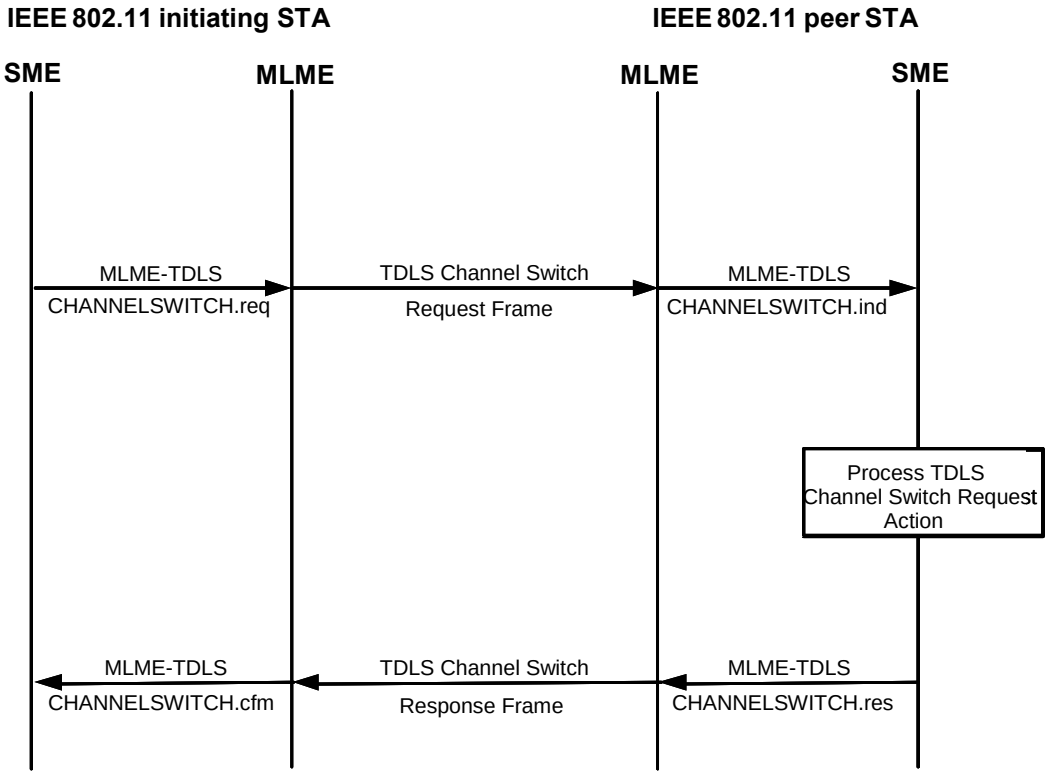

Figure 10-6d—TDLS Channel Switching

10.3.47.1 MLME-TDLSCHANNELSWITCH.request

10.3.47.1.1 Function

This primitive requests that a TDLS Channel Switch Request frame be sent to the TDLS peer STA.

10.3.47.1.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSCHANNELSWITCH.request(
                                TDLSPeerSTAAddress,
                                TDLSChannelSwitchRequest,
                                )
```

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the address of the TDLS peer MAC entity to which a TDLS Channel Switch Request frame must be transmitted.
TDLS ChannelSwitchRequest	Sequence of octets	As defined in TDLS Channel Switch Request frame	Specifies the proposed service parameters for the TDLS Channel Switch.

10.3.47.1.3 When Generated

This primitive is generated by the SME to request that a TDLS Channel Switch Request frame be sent to the TDLS peer STA.

10.3.47.1.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Channel Switch Request frame. The STA then attempts to transmit this to the TDLS peer STA.

10.3.47.2 MLME-TDLSCHANNELSWITCH.confirm

10.3.47.2.1 Function

This primitive reports the result of an MLME-TDLSCHANNELSWITCH.request primitive to switch a channel with a TDLS peer STA.

10.3.47.2.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSCHANNELSWITCH.confirm(
                        TDLSPeerSTAAddress,
                        ResultCode,
                        TDLSChannelSwitchResponse
                        )
```

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA from which a TDLS Channel Switch Response frame was received.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, UNSPECIFIED_FAILURE,	Indicates the results of the corresponding MLME-TDLSCHANNELSWITCH.request primitive.
TDLS ChannelSwitchResponse	Sequence of octets	As defined in TDLS Channel Switch Response frame	If the ResultCode was SUCCESS, specifies the proposed service parameters for the TDLS Channel Switch.

10.3.47.2.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSCHANNELSWITCH.request and indicates the results of the request.

This primitive is generated when the STA successfully receives a TDLS Channel Switch Response frame from the TDLS peer STA.

10.3.47.2.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSCHANNEL-SWITCH.request primitive and may use the reported data.

10.3.47.3 MLME-TDLSCHANNELSWITCH.indication

10.3.47.3.1 Function

This primitive indicates that a TDLS Channel Switch request frame was received from a TDLS peer STA.

10.3.47.3.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSCHANNELSWITCH.indication(
                    TDLSPeerSTAAddress,
                    TDLSChannelSwitchRequest
                    )
```

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MACAddress	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA from which a TDLS Channel Switch Request frame was received.
TDLS ChannelSwitchRequest	Sequence of octets	As defined in TDLS Channel Switch Request frame	Specifies the proposed service parameters for the TDLS Channel Switch.

10.3.47.3.3 When Generated

This primitive is generated by the MLME when a valid TDLS Channel Switch Request frame is received.

10.3.47.3.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure in 11.19.

10.3.47.4 MLME-TDLSCHANNELSWITCH.response

10.3.47.4.1 Function

This primitive requests that a TDLS Channel Switch Response frame be sent to the TDLS peer STA.

10.3.47.4.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSCHANNELSWITCH.response(
TDLSPeerSTAAddress,
TDLSChannelSwitchResponse
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA to which a TDLS Channel Switch Response frame must be transmitted.
TDLS ChannelSwitchResponse	Sequence of octets	As defined in TDLS Channel Switch Response frame	Specifies the proposed service parameters for the TDLS Channel Switch.

10.3.47.4.3 When Generated

This primitive is generated by the SME to request that a TDLS Channel Switch Response frame be sent to the TDLS peer STA.

10.3.47.4.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Channel Switch Response frame. The STA then attempts to transmit this frame to the TDLS peer STA.

10.3.48 TDLS Peer PSM

The following MLME primitives support the signaling of tunneled direct link setup. Figure 10-6e depicts the TDLS Peer PSM process. The figure is only an example of the basic procedure and is not meant to be exhaustive of all possible uses of the protocol.

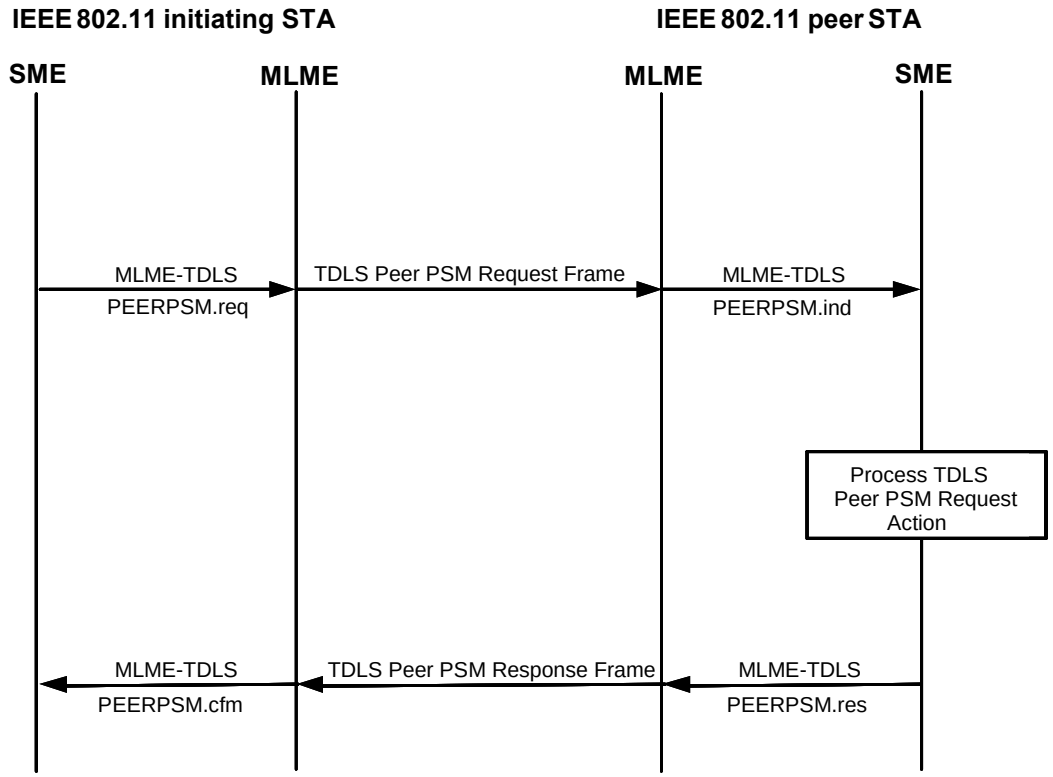

Figure 10-6e—TDLS Peer PSM

10.3.48.1 MLME-TDLSPEERPSM.request

10.3.48.1.1 Function

This primitive requests that a TDLS Peer PSM Request frame be sent to the TDLS peer STA.

10.3.48.1.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSPEERPSM.request(
TDLSPeerSTAAddress,
TDLSPeerPSMRequest
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA to which a TDLS Peer PSM Request frame must be transmitted.
TDLS PeerPSMRequest	Sequence of octets	As defined in TDLS Peer PSM Request frame	Specifies the proposed service parameters for the TDLS Peer PSM.

10.3.48.1.3 When Generated

This primitive is generated by the SME to request that a TDLS Peer PSM Request frame be sent to the TDLS peer STA.

10.3.48.1.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Peer PSM Request frame. The STA then attempts to transmit this to the TDLS peer STA.

10.3.48.2 MLME-TDLSPEERPSM.confirm

10.3.48.2.1 Function

This primitive reports the result of an MLME-TDLSPEERPSM.request primitive to initiate power save mode based on scheduled service periods with a TDLS peer STA.

10.3.48.2.2 Semantics of the Service Primitive

The primitive parameters are as follows:

```
MLME-TDLSPEERPSM.confirm(
                        TDLSPeerSTAAddress,
                        ResultCode,
                        TDLSPeerPSMResponse
                        )
```

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA from which a TDLS Peer PSM Response frame was received.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, UNSPECIFIED_FAILURE,	Indicates the results of the corresponding MLME-TDLSPEERPSM.request primitive.
TDLS PeerPSMResponse	Sequence of octets	As defined in TDLS Peer PSM Response frame	If the ResultCode was SUCCESS, specifies the proposed service parameters for the TDLS Peer PSM.

10.3.48.2.3 When Generated

This primitive is generated by the MLME as a result of an MLME-TDLSPEERPSM.request and indicates the results of the request.

This primitive is generated when the STA successfully receives a TDLS Peer PSM Response frame from the TDLS peer STA, when the MLME-TDLSPEERPSM.request contains invalid parameters, or when an unspecified failure occurs.

10.3.48.2.4 Effect of Receipt

On receipt of this primitive, the SME evaluates the results of the MLME-TDLSPEERPSM.request primitive and may use the reported data.

10.3.48.3 MLME-TDLSPEERPSM.indication

10.3.48.3.1 Function

This primitive indicates that a TDLS Peer PSM Request frame was received from a TDLS peer STA.

10.3.48.3.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSPEERPSM.indication(
TDLSPeerSTAAddress,
TDLSPeerPSMRequest
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA MAC entity from which a TDLS Peer PSM Request frame was received.
TDLSPeerPSMRequest	Sequence of octets	As defined in TDLS Peer PSM Request frame	Specifies the proposed service parameters for the TDLS Peer PSM.

10.3.48.3.3 When Generated

This primitive is generated by the MLME when a valid TDLS Peer PSM Request frame is received.

10.3.48.3.4 Effect of Receipt

On receipt of this primitive, the SME should operate according to the procedure in 11.2.1.13.

10.3.48.4 MLME-TDLSPEERPSM.response

10.3.48.4.1 Function

This primitive requests that a TDLS Peer PSM Response frame be sent to the TDLS peer STA.

10.3.48.4.2 Semantics of the Service Primitive

The primitive parameters are as follows:

MLME-TDLSPEERPSM.response(
TDLSPeerSTAAddress,
TDLSPeerPSMResponse
)

Name	Type	Valid Range	Description
TDLSPeerSTAAddress	MAC Address	Any valid individual MAC Address	Specifies the MAC address of the TDLS peer STA to which a TDLS Peer PSM Response frame must be transmitted.
TDLSPeerPSMResponse	Sequence of octets	As defined in TDLS Peer PSM Response frame	Specifies the proposed service parameters for the TDLS Peer PSM.

10.3.48.4.3 When Generated

This primitive is generated by the SME to request that a TDLS Peer PSM Response frame be sent to the TDLS peer STA.

10.3.48.4.4 Effect of Receipt

On receipt of this primitive, the MLME constructs a TDLS Peer PSM Response frame. The STA then attempts to transmit this to the TDLS peer STA.

11. MLME

11.2 Power management

11.2.1 Power management in an infrastructure network

Insert new subclauses 11.2.1.13 and 11.2.1.14 after subclause 11.2.1.12 as follows:

11.2.1.13 TDLS Peer Power Save Mode

TDLS Peer Power Save Mode (TDLS Peer PSM) is a power save mechanism that can be used between TDLS peer STAs, and which is based on a periodic wakeup schedule. A STA supports TDLS Peer PSM if dot11TDLSPeerPSMActivated is true. A STA supporting this capability may indicate support through any TDLS Setup Request frame or TDLS Setup Response frame. A STA indicating this support shall signal this by setting the TDLS Peer PSM Support subfield in the Extended Capabilities element included in the TDLS Setup Request frame or TDLS Setup Response frame to one. A station that signals support for this capability is capable of acting in both the TDLS Peer PSM initiator and the TDLS Peer PSM responder role.

A STA that intends to enter TDLS Peer PSM (TDLS Peer PSM initiator) shall send a TDLS Peer PSM Request frame to the TDLS peer STA (TDLS Peer PSM responder), including a proposed periodic Wakeup Schedule. A TDLS Peer PSM Request frame shall not be transmitted to a STA that did not indicate support for TDLS Peer PSM. When the TDLS Peer PSM responder accepts the proposed Wakeup Schedule, it shall respond with a TDLS Peer PSM Response frame indicating status code 0 (“Successful). Otherwise the TDLS Peer PSM responder shall respond with a TDLS Peer PSM Response frame indicating the appropriate status code for rejecting the schedule. An alternative schedule shall be included in the TDLS Peer PSM Response frame when the status code is set to 2 (“TDLS Wakeup Schedule rejected but alternative schedule provided”). The alternative schedule may be used by the TDLS Peer PSM initiator to generate a new TDLS Peer PSM Request frame. After successfully transmitting or receiving a TDLS Peer PSM Response frame indicating status code 0 (“Successful”), the TDLS Peer PSM initiator and TDLS Peer

PSM responder have established a periodic wakeup schedule between them. The wakeup schedule remains valid until either

- the TDLS direct link is torn down
- the STAs explicitly update the existing wakeup schedule, or
- no MPDUs containing data have been exchanged for Idle Count consecutive Awake Windows.

A STA transmitting a TDLS Peer PSM Request frame shall remain in the wake state until it received the corresponding TDLS Peer PSM Response frame. A TDLS Peer PSM Request frame may be transmitted via the AP path or via the direct path (which is up to the implementer to decide). A TDLS Peer PSM Response frame shall be transmitted over the direct path.

The timing of the periodic schedule of the TDLS Peer PSM Awake Windows is based on the Offset field, the Interval field, the Awake Window Backoff field and the Awake Window Duration field of the TDLS Peer PSM Setup Request frame that established TDLS Peer PSM operation on the link. Awake Windows begin at TSF values that satisfy the equation TSF mod Interval = Offset. The interval between the start of two successive Awake Windows is equal to the time in microseconds of the Interval field. The periodic wakeup schedule may be unrelated to the TBTT or the Beacon Interval. When the Awake Window Backoff field is set to an unsigned integer that is greater than zero, the Awake Window ends when an EDCA AC_BE backoff counter (referred to as Awake Window backoff) with an initial value equal to the value of the Awake Window backoff counter reaches zero, or when the time specified in the Awake Window Duration field has been reached, whichever is earlier. Each Awake Window associated with a different TDLS Peer PSM STA uses a separate backoff counter, and none of the counters is the EDCA AC_BE backoff counter described in 9.9.1.5 for use in determining when to transmit frames from the AC_BE queue. An Awake Window Duration field value of zero means that there is no maximum time limit and in such a case, only the expiration of the Awake Window backoff is used to determine the end of the Awake Window. When the Awake Window Backoff field is set to zero, the Awake Window ends when the time specified in the Awake Window Duration field has been reached. The Awake Window Backoff field and Awake Window Duration fields shall not both be set to zero. The Awake Window backoff starts at the beginning of the Awake Window with the value set to the value of the Awake Window Backoff field, regardless of any remaining backoff that might have existed at the end of the previous Awake Window. The Awake Window Backoff field should be set to a value that is larger than CWmin[AC_BE]. The Awake Window backoff causes the wakeup window to scale with the traffic intensity on the medium, which under busy medium conditions avoids that the wakeup window expires before the STAs have had a chance to transmit, while avoiding long wakeup windows when the medium is lightly loaded. The wake time is capped by the Awake Window Duration, so that the wake time can be limited in case of heavy interference. A fixed Awake Window can be preferred when the signal strength on the TDLS Direct Link is low and the TDLS peer STAs may experience different medium busy conditions. The Offset field contained in a TDLS Peer PSM Setup Request frame shall be set to a random value between 0 and the value of the Interval field of the TDLS Peer PSM Setup Request frame.

A TDLS Peer PSM service period is a contiguous period of time during which one or more unicast frames are transmitted between two TDLS peer STAs when at least one STA employs TDLS Peer PSM. A TDLS Peer PSM service period may be initiated during an Awake Window. A TDLS peer STA in power save mode may enter a doze state when it has successfully transmitted to and received from the corresponding TDLS peer STA in power save mode a frame with the EOSP subfield set to one, ending the TDLS Peer PSM service period. A TDLS peer STA in power save mode may enter a doze state when it has successfully received from the corresponding TDLS peer STA in active mode a frame with the EOSP subfield set to one.

Either STA may update an existing schedule by initiating a TDLS Peer PSM Request/Response exchange. If the TDLS Peer PSM Response frame indicates status code 0 (“Successful”), a new wakeup schedule is established for the TDLS direct link. Otherwise, the existing schedule still applies. The new schedule takes effect after the termination of the current TDLS Peer PSM service period.

After the successful PSM setup, a STA informs its TDLS peer STA that it will enter power save mode per direct link by setting the Power Management field to one in an MPDU requiring acknowledgement. The STA enters power save mode after successful transmission of the MPDU. The power save status on one direct link is independent of the power save status on other links (direct or with the AP) the STA may have. If a TDLS peer STA enters power save mode when a Wakeup Schedule is active, it shall be awake at the beginning of each scheduled periodic Awake Windows, and stay awake for the duration of the Awake Window or until the end of a TDLS Peer PSM service period. Otherwise, it may enter a doze state, depending on the current requirements to be awake, imposed by other links. A TDLS peer STA that did not enter power save mode shall remain in the awake state.

When both TDLS peer STAs set the More Data ACK subfield in their QoS Capability information element to one, then the More Data field inside an ACK frame set to zero shall have the same function as the EOSP subfield inside a QoS frame set to one. Transmission of an ACK frame with the More Data subfield set to zero under these conditions is equivalent to a successful transmission of a frame with the EOSP subfield set to one.

When waking up at the beginning of an Awake Window, if a STA has no buffered frame to send to a TDLS Peer STA that had the More Data Ack subfield in its QoS Capability element set to one during the TDLS setup exchange, the TDLS STA may send a QoS-Null frame with the EOSP subfield of the QoS Control field set to one, and the More Data subfield of the Frame Control field set to zero. If the TDLS peer STA that is the recipient of this QoS-Null frame has no buffered frame to deliver either, and it had the More Data Ack subfield in its QoS Capability element set to one during the TDLS setup exchange, then the TDLS peer STA shall respond with an ACK frame that has the More Data subfield set to zero. The STA may discard the QoS-Null frame if it has not been successfully transmitted at the end of the Awake Window. If a Data frame, other than the QoS-Null frame, with an EOSP subfield set to one is received from a TDLS peer STA before the successful transmission of the QoS-Null frame, the STA may cancel the pending transmission of the QoS-Null frame if it sends an ACK frame with More Data subfield set to zero in response to the received Data frame.

To keep track of the connectivity over the direct link and to maintain the wakeup schedule, TDLS peer STAs may start an acknowledged frame exchange at least once per Idle Count consecutive Awake Windows, as a keepalive. For instance a QoS-Null frame may be used as a keepalive frame. When a TDLS Peer PSM Response frame was successfully transmitted or received and no subsequent TDLS Peer PSM service period has started for Idle Count consecutive wakeup periods, the TDLS peer STAs shall delete the wakeup schedule for this link, which means that the related periodic wakeup no longer occurs (i.e. the TDLS peer STAs no longer have to wake up during this period) and that a wakeup schedule no longer exists for this link. When traffic arrives at a TDLS peer STA in TDLS Peer PSM mode for a link with no existing wakeup schedule, the STA shall send a TDLS Peer PSM Request frame through the AP path to the TDLS peer STA to activate a new wakeup schedule. When both TDLS peer STAs enter active mode while a wakeup schedule is active, no more TDLS Peer PSM service periods will occur, causing the wakeup schedule to be deleted.

If a TDLS peer STA does not receive an acknowledgment to a directed MPDU sent with the EOSP subfield set to one that terminates a TDLS Peer PSM service period, it shall retransmit that frame at least once within the same service period, subject to the applicable retry or lifetime limit. The maximum number of retransmissions within the same service period is the lesser of the maximum retry limit and the MIB attribute dot11TDLSPeerSTAMissingAckRetryLimit. If an acknowledgment to the retransmission of this last frame in the same service period is not received, the TDLS peer STA may wait until the next Awake Window to further retransmit that frame, subject to its applicable retry or lifetime limit. When the TDLS peer STA has transmitted a directed frame that terminates a TDLS Peer PSM service period then, except for

retransmissions of that frame, the TDLS peer STA shall not transmit any more frames to the TDLS peer STA until the next Awake Window.

A TDLS peer STA that has an active Wakeup Schedule shall not decrement a backoff count outside the Awake Windows, if that backoff precedes an MPDU that is destined for transmission on the related TDLS direct link.

A TDLS peer STA that has a frame within the queue for an AC to transmit to a TDLS peer STA that is in power save mode shall not decrement the backoff count for that AC outside of the Awake Windows for that recipient STA. Alternatively, the transmitting STA may maintain two backoff counters for that AC, one backoff counter that is decremented and used for transmission decisions only during Awake Windows, and a separate backoff counter that is decremented and used for transmission decisions only outside of Awake Windows. In addition to maintaining separate backoff counters, all control variables for CW incrementing and resetting decisions are duplicated.

11.2.1.14 Peer U-APSD

A STA supports the Peer U-APSD Buffer STA function if dot11TDLSPeerUAPSDBufferSTAActivated is true. A STA supporting this capability may indicate support through any TDLS Setup Request frame or TDLS Setup Response frame. A STA indicates support by setting the Peer U-APSD Buffer STA Support subfield in the Extended Capabilities element included in the TDLS Setup Request frame or TDLS Setup Response frame to one. Support for the Peer U-APSD Buffer STA function means that the STA has the capability to buffer frames destined to the PU sleep STA, and to deliver them during unscheduled service periods.

To operate as the PU Sleep STA in Peer U-APSD, a STA shall configure its Peer U-APSD capable TDLS peer STA by setting one or more U-APSD Flag subfields inside the QoS Info subfield of the QoS Capability element carried in a TDLS Setup Response frame to one, or by setting one or more U-APSD Flag subfields inside the QoS Info subfield of the EDCA Parameter Set element carried in a TDLS Setup Confirm frame to one.

A STA that configured Peer U-APSD at a TDLS peer STA enters power save mode on a TDLS direct link after the successful transmission to the TDLS peer STA over the direct link of an acknowledged MPDU with the Power Management field set to one. The STA that transmitted the frame with the Power Management field set to one is then referred to as a PU sleep STA. The STA that received the frame with the Power Management field set to one is referred to as a PU buffer STA. A PU sleep STA may be a PU buffer STA at the same time and on the same link, by sending a frame to the TDLS peer STA with the Power Management subfield of the Frame Control field set to one (possibly preceded by a TDLS Peer Traffic Indication frame). The power save status on one direct link is independent of the power save status on other links (direct or with the AP) the STA may have.

The procedure to trigger and terminate an unscheduled SP between PU buffer STA and a PU sleep STA are described in 11.2.1.4 and 11.2.1.5, where the PU buffer STA shall take the role of the AP and the PU sleep STA shall take the role of the non-AP STA using U-APSD.

11.2.1.14.1 Peer U-APSD Behavior at the PU buffer STA

MSDUs at a PU buffer STA destined for a PU sleep STA shall be temporarily buffered at the PU buffer STA. The algorithm to manage this buffering is beyond the scope of this standard, except that the PU buffer STA shall preserve the order of frames on a per-TID, per-STA basis.

A PU buffer STA shall transmit a unicast TDLS Peer Traffic Indication frame to a PU sleep STA, through the AP, if and only if all of the following conditions are met:

- a frame with an RA corresponding to a PU sleep STA is placed into a buffer at the PU buffer STA,
- the buffer into which the frame was placed contained no other frames with the same RA, and
- a period of dot11TDLSPeerUAPSDIndicationWindow Beacon Intervals has expired after the last service period.

The TDLS Peer Traffic Indication frame shall be transmitted through the AP path.

The transmitted TDLS Peer Traffic Indication frame shall indicate the non-empty AC(s), by setting the corresponding AC Traffic Available subfield of the TDLS Peer Traffic Indication frame to one.

A PTI Control element may be included in the TDLS Peer Traffic Indication frame, to allow the PU sleep STA to not start a service period when the indicated traffic has already been received by the PU sleep STA.

The TID field of the PTI Control element (if included) shall be set to the highest TID for which the PU buffer STA has traffic buffered that is destined to the PU sleep STA to which the TID field will be transmitted.

The Sequence Control field contained in the PTI Control element is set to the sequence number of the latest MPDU that has been transmitted over the TDLS direct link to the PU sleep STA that is the destination of the TDLS Peer Traffic Indication frame that contains the PTI Control element. The TID field contained in the PTI Control element is set to the TID of that MPDU.

After transmitting a TDLS Peer Traffic Indication frame, the PU buffer STA shall stay awake at least until the corresponding TDLS Peer Traffic Response frame is received.

After transmitting a TDLS Peer Traffic Indication frame with a PTI Control element, the PU buffer STA shall stay awake at least until the MPDU following the MPDU indicated in the Sequence Control field of the PTI Control element is successfully transmitted.

11.2.1.14.2 Peer U-APSD Behavior at the PU sleep STA

When a PU sleep STA receives a TDLS Peer Traffic Indication frame without a PTI Control element, the PU sleep STA shall initiate a service period with the PU buffer STA during which it shall transmit at least a TDLS Peer Traffic Response frame. The TDLS Peer Traffic Response frame shall echo the Dialog Token and the Link Identifier from the corresponding TDLS Peer Traffic Indication frame.

When a PU sleep STA receives a TDLS Peer Traffic Indication frame with a PTI Control element, and the PU sleep STA has not received from the PU buffer STA the MPDU following the MPDU that is indicated in the TDLS Peer Traffic Indication frame, the PU sleep STA shall initiate a service period with the PU buffer STA to retrieve the buffered traffic for the AC(s) for which no unscheduled SP is currently active.

11.4 TS operation

11.4.1 Introduction

Change the 6th paragraph of 11.4.1 as follows:

In the direct-link or TDLS direct link case, it is the responsibility of the non-AP STA that is going to send the data to create the TS. A Direct Link TS is unidirectional.

Insert a new subclause 11.19 after subclause 11.18 as follows:

11.19 Tunneled Direct Link Setup

11.19.1 General

Tunneled Direct Link Setup (TDLS) is characterized by encapsulating setup frames in Data frames, which allows them to be transmitted through an AP transparently. Therefore, the AP does not need to be direct link capable, nor does it have to support the same set of capabilities that will be used on the direct link between the two TDLS peer STAs. TDLS also includes power saving, in the form of TDLS Peer PSM (scheduled) and Peer U-APSD (unscheduled). STAs that set up a TDLS direct link remain associated with their BSS, but have the option of transmitting frames directly to the other TDLS peer STA.

Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA.

To set up and maintain a direct link, both TDLS peer STAs shall be associated with the same infrastructure BSS.

A TDLS peer STA may be involved in direct links with multiple TDLS peer STAs at the same time. Simultaneous operation of DLS and TDLS between the same pair of STAs is not allowed. A DLS Request frame shall not be transmitted to a STA with which a TDLS direct link is currently active. A DLS Request frame received from a STA with which a TDLS direct link is currently active shall be discarded.

The channel on which the AP operates is referred to as the base channel. If the AP operates in a 40 MHz channel, then the base channel refers to the primary channel. If the direct link is switched to a channel that is not the base channel, then this channel is referred to as the off-channel.

Features that are not supported by the BSS but that are supported by both TDLS peer STAs may be used on a TDLS direct link between those STAs, except PCO. An example is the use of an HT MCS on a TDLS direct link between HT STAs when these STAs are associated with a non-HT BSS. Features that are supported by the BSS shall follow the BSS rules when they are used on a TDLS direct link on the base channel. The channel width of the TDLS direct link on the base channel shall not exceed the channel width of the BSS to which the TDLS peer STAs are associated.

When admission control is required for an AC on the base channel, then the TDLS peer STA that intends to use this AC for direct link transmissions on the base channel is responsible for setting up an appropriate TS with the AP, as defined in 9.9.3.1.

A non-AP STA may act as TDLS initiator STA or TDLS responder STA when dot11TunneledDirectLink-SetupImplemented is true.

TDLS frames shall use the formatting as specified in 11.19.1 when they are transmitted through the AP and when they are transmitted over the TDLS direct link. A STA shall not transmit a TDLS Action frame with the Type field of the frame set to Management. A received TDLS Action frame with the Type field set to Management shall be discarded.

TDLS shall not be used in an IBSS.

Security is only available on the TDLS direct link when both TDLS peer STAs have an RSNA with the BSS.

TDLS shall not be used when the TDLS Prohibited subfield included in the Extended Capability element of the Association Response frame or Reassociation Response frame that led to the current association is set to one.

11.19.2 TDLS payload

TDLS uses Ethertype 89-0d frames, as defined in Annex U. The TDLS payload contains a TDLS Action frame body as is specified in 7.4.11. The UP shall be AC_VI, unless otherwise specified.

11.19.3 TDLS Discovery

To discover TDLS capable STAs in the same BSS, a TDLS initiator STA sends a TDLS Discovery Request frame to a unicast DA or to the Broadcast DA, through the AP. When the TDLS Discovery Request frame is sent to the Broadcast address, the TDLS responder STA Address field contained in the Link Identifier element of the TDLS Discovery Request frame shall be set to the Broadcast address. A TDLS capable STA that receives a TDLS Discovery Request frame with a matching BSSID in the BSSID element (TDLS responder STA) shall send a TDLS Discovery Response frame to the requesting STA, via the direct path. The TDLS responder STA Address field contained in the Link Identifier element of the TDLS Discovery Response frame shall be set to the MAC address of the STA sending the TDLS Discovery Response frame. The TDLS Discovery Response frame shall be sent using AC_BE when the TDLS responder STA Address field contained in the Link Identifier element of the TDLS Discovery Request frame indicates the Broadcast address.

A TDLS STA may also send TDLS Setup Request frame to a STA in the same BSS to discover whether the peer STA is TDLS capable or not. A TDLS Setup Response frame in response to TDLS Setup Request frame indicates peer STA sending TDLS Setup Response TDLS capable.

11.19.4 TDLS Direct Link Establishment

To establish a TDLS direct link, the TDLS initiator STA shall send a TDLS Setup Request frame to the intended TDLS responder STA.

TDLS Setup Request frames, TDLS Setup Response frames and TDLS Setup Confirm frames shall be transmitted through the AP.

Upon receipt of a TDLS Setup Request frame, the following options exist at the TDLS responder STA:

1. The TDLS responder STA accepts the TDLS Setup Request frame, in which case the TDLS responder STA shall respond with a TDLS Setup Response frame with status code 0 (“Successful”).

2. The TDLS responder STA declines the TDLS Setup Request frame, in which case the TDLS responder STA shall respond with a TDLS Setup Response frame with status code 37 ("The request has been declined"). A TDLS setup request shall be declined when the BSSID in the received Link Identifier does not match the BSSID of the TDLS responder STA.

3. The TDLS Setup Request frame is received after sending a TDLS Setup Request frame and before receiving the corresponding TDLS Setup Response frame, and the source address of the received TDLS Setup Request frame is higher than its own MAC address, in which case the TDLS responder STA shall discard the message and the TDLS responder STA shall send no TDLS Setup Response frame.

4. The TDLS Setup Request frame is received after sending a TDLS Setup Request frame and before receiving the corresponding TDLS Setup Response frame, and the source address of the received TDLS Setup Request frame is lower than its own MAC address. In this case, the TDLS responder STA shall terminate the TDLS setup it initiated. The TDLS responder STA shall send a response according to item 1 or 2 above in this case.

5. If a TDLS Setup Request frame is received from a TDLS responder STA with which a currently active TDLS session exists, then the receiving STA shall discard the received TDLS Setup Request frame.

If no TDLS Setup Response frame is received within dot11TDLSResponseTimeout, or if a TDLS Setup Response frame is received with a non-zero status code, the TDLS initiator STA shall terminate the setup procedure and discard the TDLS Setup Response frame. Otherwise, the TDLS initiator STA shall send a TDLS Setup Confirm frame to the TDLS responder STA to confirm the receipt of the TDLS Setup Response frame.

The EDCA Parameter Set element inside the TDLS Setup Confirm frame shall contain the QoS parameters that shall be used by the TDLS peer STAs on the off–channel, and on the base channel when the BSS is not QoS capable, and/or on the off-channel. The ACM subfields inside the EDCA Parameter Set element shall be set to 0. When the BSS is QoS capable, then the BSS QoS parameters shall be used by the TDLS peer STAs on the base channel, and the values indicated inside the TDLS Setup Confirm frame apply only for the off-channel.

If dot11RSNAEnabled is true, then the TPK Handshake messages will be included in the TDLS Setup messages, as follows:

- TPK Handshake Message 1 shall be included in the TDLS Setup Request frame
- TPK Handshake Message 2 shall be included in the TDLS Setup Response frame
- TPK Handshake Message 3 shall be included in the TDLS Setup Confirm frame

When the TDLS Setup Handshake has been completed, the TDLS initiator STA and the TDLS responder STA are TDLS peer STAs. A TDLS peer STA shall accept data frames received from the respective TDLS peer STA directly and Data frames destined for the respective TDLS peer STA may be transmitted over the direct link.

Subsequent to the successful completion of the TPK Handshake, all frames transmitted and received on the TDLS direct link shall be protected using the TPKSA, per the procedures defined in Clause 8.

An AP may discard TDLS Setup Request frames to prevent direct links from being set up in its BSS. In this case, the AP may send a TDLS Setup Response frame with status code 4 "Direct links not allowed by the BSS" to the sender of the TDLS Setup Request frame. The AP shall insert into the Address 3 field of the

TDLS Setup Response frame the TDLS responder STA Address from the Link Identifier element in the TDLS Setup Request frame.

A TDLS Setup Request frame received at a STA that does not support TDLS shall be ignored.

To avoid possible reordering of MSDUs, a TDLS initiator STA shall cease transmitting MSDUs to the TDLS responder STA through the AP after sending a TDLS Setup Request frame, and a TDLS responder STA shall cease transmitting MSDUs to the TDLS initiator STA through the AP after sending a TDLS Setup Response frame indicating status code 0 (Success).

The TDLS Setup Request frame and the TDLS Setup Response frame shall be transmitted using the lowest AC that was used for transmitting MSDUs to the respective TDLS peer STA during the past INTERVAL, or at AC_BK. When no MSDUs were transmitted during the INTERVAL, then the TDLS Setup Request frame and the TDLS Setup Response frame may be sent at any AC, subject to applicable Admission Control rules.

If no TDLS Setup Response frame is received within dot11TDLSResponseTimeout, or if a TDLS Setup Response frame is received with status code other than 0 (“Success”), the TDLS initiator STA may resume transmitting MSDUs to the TDLS responder STA through the AP.

If a TDLS Setup Confirm frame is transmitted with a status code other than 0 (“Success”), the TDLS initiator STA may resume transmitting MSDUs to the TDLS responder STA through the AP.

If a TDLS Setup Confirm frame is received with a status code other than 0 (“Success”), the TDLS responder STA may resume transmitting MSDUs to the TDLS initiator STA through the AP.

A TDLS peer STA shall not transmit MSDUs over the direct link before transmitting or receiving a TDLS Setup Confirm frame with status code 0 (“Success”).

11.19.5 TDLS Direct Link Teardown

To tear down a direct link, a TDLS peer STA shall send a TDLS Teardown frame to the respective TDLS peer STA. A TDLS peer STA shall disable the direct link and destroy the related security parameters after successfully transmitting or receiving a TDLS Teardown frame. If dot11RSNAEnabled is true, then the FTIE shall be included in the TDLS Teardown frame.

The TDLS Teardown frame shall be sent over the direct path and the reason code shall be set to “TDLS direct link teardown for unspecified reason”, except when the TDLS peer STA is unreachable via the TDLS direct link, in which case, the TDLS Teardown frame shall be sent through the AP and the reason code shall be set to “TDLS direct link teardown due to TDLS peer STA unreachable via the TDLS direct link”. If the direct link is on an off-channel when this condition occurs, then the TDLS peer STA may switch back to the base channel without initiating a channel switch frame exchange, before transmitting the TDLS Teardown frame.

If present, the contents of the FTIE in the TDLS Teardown frame shall be the same as that included in the TPK Handshake Message 3 with the exception of the MIC field. The MIC shall be calculated on the concatenation, in the following order, of:

- Link Identifier element
- Reason Code
- Dialog token

- Transaction Sequence number (1 octet) which shall be set to the value 4
- FTIE, with the MIC field of the FTIE set to 0

If dot11RSNAEnabled is true and TPK Handshake was successful for this TDLS session, then a receiving STA shall validate the MIC in the TDLS Teardown frame prior to processing the TDLS Teardown frame. If MIC validation fails, the receiver shall ignore the TDLS Teardown frame.

When a TDLS Direct Link gets torn down, any related TSs shall be deleted by the TDLS peer STAs.

A TDLS Teardown frame shall be transmitted to all current TDLS peer STAs (via the AP or via the direct path) prior to transmitting a Disassociation frame or a Deauthentication frame to the AP.

11.19.6 TDLS Channel Switching

When a STA enables support for TDLS channel switching, it shall set dot11TDLSChannelSwitching-Activated, dot11MultiDomainCapabilityEnabled and dot11ExtendedChannelSwitchEnabled to true. When TDLS channel switching is enabled, the STA may set TDLS Channel Switching capability field to one. The STA shall include a Supported Channels element and a Supported Regulatory Classes element in all TDLS Setup Request and TDLS Setup Response frames that have a TDLS Channel Switching capability field set to one. A channel switch shall not be initiated by a STA when the TDLS peer STA did not set the TDLS Channel Switching capability field to one in the transmitted TDLS Setup Request frame or the TDLS Setup Response frame that caused the TDLS direct link to be set up.

TDLS Channel Switch Request frames and TDLS Channel Switch Response frames shall be transmitted over the TDLS direct link.

TDLS channel switching is different from (I)BSS channel switching as defined in 11.9.7.

The channel on which the AP operates is referred to as the base channel. If the AP operates in a 40 MHz channel, then the base channel refers to the primary channel. If the direct link is switched to a channel that is not the base channel, then this channel is referred to as the off-channel.

The target channel is the destination channel of an intended channel switch. The target channel is specified by the STA that initiates a channel switch, from the set of regulatory classes supported by both TDLS peer STAs. The target channel and regulatory class are specified in the TDLS Channel Switch Request frame. The Country and Coverage Class settings on the target channel are the same as in the BSS to which both TDLS peer STAs are currently associated. Both STAs are entitled to request a channel switch. The events occurring for a channel switch are illustrated in Figure 11-17b.

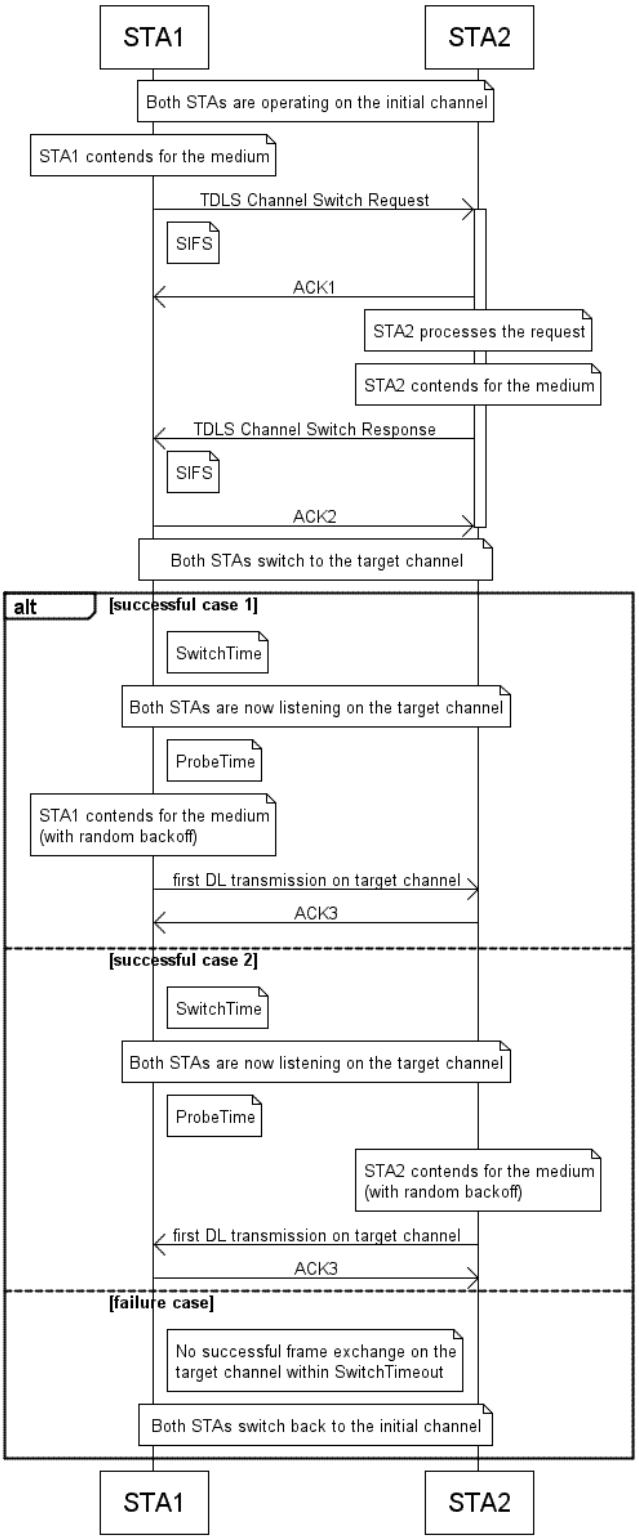

Figure 11-17b—Events occurring for a TDLS direct link channel switch

In Figure 11-17b, the TDLS peer STAs (STA1 and STA2) are operating on an initial channel. After contending for the medium, STA1 transmits a TDLS Channel Switch Request frame to STA2, via the direct link, indicating a requested switch to a target channel. STA2 transmits an ACK frame (denoted ACK1 in Figure 11-17b) after SIFS, and processes the TDLS Channel Switch Request frame. After contending for the medium, STA2 transmits a TDLS Channel Switch Response frame to STA1, possibly also after entering power save mode with the AP. STA1 responds with an ACK frame (denoted ACK2 in Figure 11-17b) after SIFS. If the TDLS Channel Switch Response frame indicated with status code 37 ("The request has been declined"), then both STAs continue to operate on the current channel. If the TDLS Channel Switch Response frame indicated with status code 0 ("Successful"), then both STAs shall be listening on the target channel not later than SwitchTime after the end of the last symbol of ACK2, as measured at the air interface. After switching channels, each TDLS peer STA shall perform a clear channel assessment (CCA) on the target channel, until a frame sequence is detected by which it can correctly set its NAV, or until a period of time equal to at least dot11TDLSProbeDelay has transpired (this combined event is indicated as "ProbeTime" in Figure 11-17b). The first transmission on the target channel shall be preceded by a random backoff, which shall start at the end of the ProbeTime. The first transmission on the new channel shall not start before the end of SwitchTime. The initiator of the channel switch shall transmit a Data frame on the target channel, unless the SwitchTimeout has expired or the responder to the channel switch transmitted a Data frame on the target channel.

If no successful frame exchange has occurred on an off-channel within SwitchTimeout after the end of the last symbol of ACK2, as measured at the air interface, the STAs shall go back to the base channel, where they shall be listening not later than SwitchTime after the end of the SwitchTimeout. After changing channels (either from the base channel to the off-channel or from the off-channel to the base channel), a TDLS peer STA shall perform CCA until a frame sequence is detected by which it can correctly set its NAV, or until a period of time equal to the ProbeTime has transpired.

Both the TDLS Channel Switch Request frame and the TDLS Channel Switch Response frame shall contain a Channel Switch Timing element. The SwitchTime and SwitchTimeout values in the TDLS Channel Switch Timing element included in the TDLS Channel Switch Request frame shall specify the values required at the STA sending the TDLS Channel Switch Request frame. The SwitchTime and SwitchTimeout values specified in the TDLS Channel Switch Timing element included in the TDLS Channel Switch Response frame shall meet the requirements at the STA sending the TDLS Channel Switch Response frame and shall be equal to or larger than the values specified in the TDLS Channel Switch Request frame. The timing parameters specified in the Channel Switch Timing element included in the TDLS Channel Switch Response frame shall be used for the TDLS channel switching procedure. This procedure causes the larger of the two switch times to become the value that is transmitted in the TDLS Channel Switch Response frame.

The TDLS peer STA shall be in PS mode with the AP and shall not be involved in an active Service Period with the AP before sending a TDLS Channel Switch Request frame or a TDLS Channel Switch Response frame with Status Code set to 0 ("Successful"). The TDLS peer STA that receives a TDLS Channel Switch Request frame may enter PS mode with the AP prior to sending the TDLS Channel Switch Response frame.

Because there is at least a backoff between the TDLS Channel Switch Request frame and the TDLS Channel Switch Response frame, there is a (small) probability that two STAs issue a TDLS Channel Switch Request frame at more or less the same time. To reduce the probability for this event to occur, a TDLS peer STA should not transmit a TDLS Channel Switch Request when a TDLS Channel Switch Request frame is received and no TDLS Channel Switch Response has been transmitted in response. When two TDLS Channel Switch Request frames still cross, then both TDLS Channel Switch Response frames will be executed sequentially depending on their reason code. If a TDLS Channel Switch Response frame does not imply a channel switch because the STAs already are on the requested channel, then the SwitchTime and ProbeTime may be skipped and both TDLS peer STAs continue to operate on the requested channel. To cross means that a TDLS Channel Switch Request frame is received from a TDLS peer STA after

transmitting a TDLS Channel Switch Request frame to the TDLS peer STA, instead of the expected TDLS Channel Switch Response frame.

When a TDLS peer STA does not receive an acknowledgment to a TDLS Channel Switch Response frame, it may retransmit the frame but the number of retransmissions shall be lesser of the maximum retry limit and dot11TDLSPeerSTAMissingAckRetryLimit.

A channel switch from an off-channel to the base channel may be accomplished by sending a TDLS Channel Switch Response frame indicating the base channel as the target channel, without prior TDLS Channel Switch Response frame. The Channel Switch Timing element shall be the same as contained in the Channel Switch Response frame that caused the switch to the off-channel.

TDLS Channel Switching shall not be used when the TDLS Channel Switching Prohibited subfield included in the Extended Capability element of the Association Response frame or Reassociation Response frame that led to the current association is set to one.

11.19.6.1 General Behavior on the Off-Channel

If dot11SpectrumManagementRequired is true, a TDLS peer STA shall not transmit a TDLS Channel Switch request specifying an off-channel where radar detection is required, unless the STA has tested that channel for the presence of radars according to regulatory requirements. If a TDLS peer STA that is operating in such a channel detects radar, the TDLS peer STA should discontinue transmissions according to regulatory requirements, and it shall send a TDLS Channel Switch Request indicating a switch to the base channel. The channel switch avoids an interruption on the direct link.

The TDLS peer STA initiating the switch to the channel where radar detection is required shall be the DFS owner.

If the TDLS Setup Confirm frame that led to the direct link on the off-channel contained an EDCA Parameter Set element, then EDCA shall be used on the off-channel, with the parameters as specified in the cited EDCA Parameter Set element. The EDCA parameters for the off-channel should be the same as those on the base channel when QoS is supported by the BSS because this may optimize the TDLS channel switching process.

The secondary channel of an existing 40 MHz network shall not be selected as an off-channel.

On an off-channel, the TDLS peer STAs remain associated with their BSS, so the BSSID remains the same.

It is recommended that in general TDLS STAs propose target channels that have no detectable medium occupancy. If no such channel is available, then it is recommended that the TDLS STA propose a target channel where beacons are detected but with little or no additional medium occupancy. It is further recommended that TDLS STAs do not propose a target channel where the presence of beacons indicate that ACM bits are set, unless little or no additional medium occupancy is detected.

11.19.6.2 Setting up a 40 MHz direct link

A 40 MHz off-channel direct link may be started if both TDLS peer STAs indicated 40 MHz support in the Supported Channel Width Set field of the HT Capabilities element (which is included in the TDLS Setup Request frame and the TDLS Setup Response frame).

Switching to a 40 MHz off-channel direct link is achieved by including the following information in the TDLS Channel Switch Request:

- Regulatory Class element indicating 40 MHz Channel Spacing
- Secondary Channel Offset element indicating SCA or SCB

The regulatory class shall not have a value of 2.407 GHz for the Channel starting frequency.

The TDLS peer STA initiating the switch to the 40 MHz off-channel shall be the IDO STA.

11.19.5.2.1 Basic 40 MHz functionality

TDLS peer STAs may transmit 40 MHz PPDUs on a 40 MHz direct link. A TDLS peer STA shall not transmit a 20 MHz PPDU in the secondary channel of its 40 MHz direct link.

11.19.6.2.2 Channel selection for a 40 MHz direct link

If a TDLS peer STA chooses to start a 40 MHz direct link that occupies the same two channels as an existing 40 MHz network (i.e. a 20/40 MHz BSSs or a 40 MHz direct link), then it shall ensure that the primary and secondary channels of the new direct link are identical to the primary and secondary channels of the existing 40 MHz network, unless the TDLS peer STA discovers that on these two channels there are existing 40 MHz networks with different primary and secondary channels.

If a TDLS peer STA chooses to start a 40 MHz direct link, the selected secondary channel should correspond to a channel on which no beacons are detected.

11.19.6.2.3 Switching from a 40 MHz to a 20 MHz direct link

Switching from a 40 MHz off-channel direct link to a 20 MHz off-channel direct link is established through a TDLS channel switch. When on a 40 MHz off-channel direct link, a requested switch to a 20 MHz direct link shall always be accepted.

11.19.6.2.4 CCA sensing and NAV assertion in a 40 MHz direct link

When active on a 40 MHz direct link, the TDLS peer STAs shall follow the CCA rules as defined in 11.14.9 and the NAV rules as defined in 11.14.10.

11.19.6.3 TDLS Channel Switching and Power Saving

A TDLS direct link may be switched to an off-channel during a Peer U-APSD service period. When no active service period exists between two TDLS peer STAs, a new service period shall start on the base channel.

A TDLS direct link may be switched to an off-channel when TDLS Peer PSM is active on the link. The wakeup windows occur on the off-channel in the same way they would have occurred had the STAs remained on the base channel. Suspension of the wakeup windows implies a switch back to the base channel.

11A. Fast BSS transition

11A.10 Remote request broker communication

11A.10.3 Remote request/response frame definition

Change the text in 11A.10.3 as follows:

This subclause defines a mechanism to transport the remote request and remote response between the current AP and the target AP. Any other mechanism may be used.

The Remote Request frame is transmitted over the DS from the current AP to the target AP. The ~~frame format~~Payload for the Remote Request/Response frame is given in Figure 11A-20. Remote Request/Response frames will use an Ethertype of 89-0d, as specified in Annex U. The Remote Request/Response frame contains version, type, and length fields, along with the AP Address

~~The Remote Frame Type for FT Remote request/response messages shall be set to 1. Received messages with Remote Frame Type other than 1 shall be discarded.~~

In Figure 11A-20, delete the first row after the table header and change the figure caption as shown:

Size	Information
~~1~~	~~Remote Frame Type~~
1	FT Packet Type
2	FT Action Length
6	AP Address
variable	FT Action Frame

Figure 11A-20—Remote Request/Response Payload~~frame~~ format

Annex A (normative) Protocol Implementation Conformance (PICS) proforma

A.4 PICS proforma–IEEE Std 802.11-2007

A.4.3 IUT configuration

Insert entry CF17 to the end of the IUT configuration table:

Item	IUT configuration	References	Status	Support
*CF17	Is Tunneled Direct Link Setup supported?	11.19	O	Yes ☐ No ☐ N/A ☐

Insert a new subclause at A.4.21 the end of A.4 as follows:

A.4.21 Tunneled Direct Link Setup extensions

Item	Protocol Capability	References	Status	Support
TDLS1	Tunneled Direct Link Setup	7.4.11, 11.19	CF2&CF17:M	Yes ☐ No ☐ N/A ☐
TDLS1.1	TDLS Setup	7.3.2.61, 7.4.11.1, 7.4.11.2, 7.4.11.3, 11.19.4	CF2&CF17:M	Yes ☐ No ☐ N/A ☐
TDLS1.2	TDLS Teardown	7.3.2.61, 7.4.11.4, 11.19.5	CF2&CF17:M	Yes ☐ No ☐ N/A ☐
TDLS1.3	TDLS Peer Key Handshake	8.5.9	CF2&CF17:M	Yes ☐ No ☐ N/A ☐
TDLS1.4	TDLS Peer PSM	7.3.2.61, 7.3.2.62, 7.4.11.8, 7.4.11.9 11.2.1.13	CF2&CF17:O	Yes ☐ No ☐ N/A ☐
TDLS1.5	TDLS Peer U-APSD	7.3.2.61, 7.3.2.64, 7.3.2.65, 7.4.11.5, 7.4.11.12 11.2.1.14	CF2&CF17:O	Yes ☐ No ☐ N/A ☐
TDLS1.6	TDLS Channel Switching	7.3.2.61, 7.3.2.63, 7.4.11.6, 7.4.11.7, 11.19.6	CF2&CF8& CF11&CF17:O	Yes ☐ No ☐ N/A ☐

Annex D (normative) ASN.1 encoding of the MAC and PHY MIB

Change the "Dot11StationConfigEntry" of the "dotStationConfig TABLE" as follows:

```
-- ****************************************************************
-- * dotStationConfig TABLE
-- ****************************************************************

Dot11StationConfigEntry ::=
SEQUENCE {
      dot11StationID                                MacAddress,
      dot11MediumOccupancyLimit                     INTEGER,
      dot11CFPollable                               TruthValue,
      dot11CFPeriod                                 INTEGER,
      dot11CFPMaxDuration                           INTEGER,
      dot11AuthenticationResponseTimeOut            Unsigned32,
      dot11PrivacyOptionImplemented                 TruthValue,
      dot11PowerManagementMode                      INTEGER,
      dot11DesiredSSID                              OCTET STRING,
      dot11DesiredBSSType                           INTEGER,
      dot11OperationalRateSet                       OCTET STRING,
      dot11BeaconPeriod                             INTEGER,
      dot11DTIMPeriod                               INTEGER,
      dot11AssociationResponseTimeOut               Unsigned32,
      dot11DisassociateReason                       INTEGER,
      dot11DisassociateStation                      MacAddress,
      dot11DeauthenticateReason                     INTEGER,
      dot11DeauthenticateStation                    MacAddress,
      dot11AuthenticateFailStatus                   INTEGER,
      dot11AuthenticateFailStation                  MacAddress,
      dot11MultiDomainCapabilityImplemented         TruthValue,
      dot11MultiDomainCapabilityEnabled             TruthValue,
      dot11CountryString                            OCTET STRING,
      dot11SpectrumManagementImplemented            TruthValue,
      dot11SpectrumManagementRequired               TruthValue,
      dot11RSNAOptionImplemented                    TruthValue,
      dot11RSNAPreauthenticationImplemented         TruthValue,
      dot11RegulatoryClassesImplemented             TruthValue,
      dot11RegulatoryClassesRequired                TruthValue,
      dot11QosOptionImplemented                     TruthValue,
      dot11ImmediateBlockAckOptionImplemented       TruthValue,
      dot11DelayedBlockAckOptionImplemented         TruthValue,
      dot11DirectOptionImplemented                  TruthValue,
      dot11APSDOptionImplemented                    TruthValue,
      dot11QAckOptionImplemented                    TruthValue,
      dot11QBSSLoadOptionImplemented                TruthValue,
      dot11QueueRequestOptionImplemented            TruthValue,
      dot11TXOPRequestOptionImplemented             TruthValue,
      dot11MoreDataAckOptionImplemented             TruthValue,
      dot11AssociatedinNQBSS                        TruthValue,
```

```
        dot11DLSAllowdInQBSS                                TruthValue,
        dot11DLSAllowed                                     TruthValue,
        dot11AssociateStation                               MacAddress,
        dot11AssociateID                                    INTEGER,
        dot11AssociateFailStation                           MacAddress,
        dot11AssociateFailStatus                            INTEGER,
        dot11ReassociateStation                             MacAddress,
        dot11ReassociateID                                  INTEGER,
        dot11ReassociateFailStation                         MacAddress,
        dot11ReassociateFailStatus                          INTEGER,
        dot11RadioMeasurementCapable                        TruthValue,
        dot11RadioMeasurementEnabled                        TruthValue,
        dot11RRMMeasurementProbeDelay                       INTEGER,
        dot11RRMMeasurementPilotPeriod                      INTEGER,
        dot11RRMLinkMeasurementEnabled                      TruthValue,
        dot11RRMNeighborReportEnabled                       TruthValue,
        dot11RRMParallelMeasurementsEnabled                 TruthValue,
        dot11RRMRepeatedMeasurementsEnabled                 TruthValue,
        dot11RRMBeaconPassiveMeasurementEnabled             TruthValue,
        dot11RRMBeaconActiveMeasurementEnabled              TruthValue,
        dot11RRMBeaconTableMeasurementEnabled               TruthValue,
        dot11RRMBeaconMeasurementReportingConditionsEnabled  TruthValue,
        dot11RRMFrameMeasurementEnabled                     TruthValue,
        dot11RRMChannelLoadMeasurementEnabled               TruthValue,
        dot11RRMNoiseHistogramMeasurementEnabled            TruthValue
        dot11RRMStatisticsMeasaurementEnabled               TruthValue,
        dot11RRMLCIMeasurementEnabled                       TruthValue,
        dot11RRMLCIAzimuthEnabled                           TruthValue,
        dot11RRMTransmitStreamCategoryMeasurementEnabled    TruthValue,
        dot11RRMTriggeredTransmitStreamCategoryMeasurementEnabled
        TruthValue,
        dot11RRMAPChannelReportEnabled                      TruthValue,
        dot11RRMMIBEnabled                                  TruthValue,
        dot11RRMMaxMeasurementDuration                      Unsigned32,
        dot11RRMNonOperatingChannelMaxMeasurementDuration   Unsigned32,
        dot11RRMMeasurementPilotTransmissionInformationEnabled TruthValue,
        dot11RRMMeasurementPilotCapability                  Unsigned32,
        dot11RRMNeighborReportTSFOffsetEnabled              TruthValue,
        dot11RRMRCPIMeasurementEnabled                      TruthValue,
        dot11RRMRSNIMeasurementEnabled                      TruthValue,
        dot11RRMBSSAverageAccessDelayEnabled                TruthValue,
        dot11RRMBSSAvailableAdmissionCapacityEnabled        TruthValue,
        dot11RRMAntennaInformationEnabled                   TruthValue,
        dot11FastBSSTransitionImplemented                   TruthValue
        dot11LCIDSEImplemented                              TruthValue,
        dot11LCIDSERequired                                 TruthValue,
        dot11DSERequired                                    TruthValue,
        dot11ExtendedChannelSwitchEnabled                   TruthValue,
        dot11RSNAProtectedManagementFramesEnabled           TruthValue,
        dot11RSNAUnprotectedManagementFramesAllowed         TruthValue,
        dot11AssociationPingResponseTimeout                 Unsigned32,
        dot11AssociationMaximumPingAttempts                 INTEGER,
        dot11HighThroughputOptionImplemented                TruthValue,
        dot11TunneledDirectLinkSetupImplemented             TruthValue,
```

```
        dot11TDLSPeerUAPSDBufferSTAActivated                TruthValue,
        dot11TDLSPeerPSMActivated                           TruthValue,
        dot11TDLSPeerUAPSDIndicationWindow                  INTEGER,
        dot11TDLSChannelSwitchingActivated                  TruthValue,
        dot11TDLSPeerSTAMissingAckRetryLimit                INTEGER,
        dot11TDLSResponseTimeout                            INTEGER,
        dot11TDLSProbeDelay                                 INTEGER
}
```

Insert seven new elements at the end of the dot11StationConfigTable element definitions:

```
dot11TunneledDirectLinkSetupImplemented OBJECT-TYPE
       SYNTAX TruthValue
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "This attribute, when TRUE, indicates that the STA
              implementation is capable of supporting Tunneled Direct
              Link Setup."
       DEFVAL { false }
       ::= { dot11StationConfigEntry 94 }

dot11TDLSPeerUAPSDBufferSTAActivated OBJECT-TYPE
       SYNTAX TruthValue
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "This attribute, when TRUE, indicates that the STA
              implementation is capable of supporting TDLS Peer U-APSD."
       DEFVAL { false }
       ::= { dot11StationConfigEntry 95 }

dot11TDLSPeerPSMActivated OBJECT-TYPE
       SYNTAX TruthValue
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "This attribute, when TRUE, indicates that the STA
              implementation is capable of supporting TDLS Peer PSM."
       DEFVAL { false }
       ::= { dot11StationConfigEntry 96 }

dot11TDLSPeerUAPSDIndicationWindow OBJECT-TYPE
       SYNTAX INTEGER (1..256)
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
              "This attribute indicates the minimum interval in Beacon Intervals
              between successive Peer Traffic Indication frames."
       DEFVAL { 1 }
```

```
        ::= { dot11StationConfigEntry 97 }

dot11TDLSChannelSwitchingActivated OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This attribute, when TRUE, indicates that the STA
                implementation is capable of supporting TDLS Channel Switching."
        DEFVAL { false }
        ::= { dot11StationConfigEntry 98 }

dot11TDLSPeerSTAMissingAckRetryLimit OBJECT-TYPE
        SYNTAX INTEGER (1..100)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute indicates the number of times the TDLS STA may retry a frame
                for which it does not receive an ACK from TDLS peer STA in power-save mode
                after the TDLS peer STA does not receive an ACK to a directed MPDU sent with
                the EOSP set to 1 or to a directed MPDU that initiated a channel switch"
        DEFVAL { 3 }
::= { dot11StationConfigEntry 99 }

dot11TDLSResponseTimeout OBJECT-TYPE
        SYNTAX INTEGER (1..65535)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute indicates the amount of time in units of seconds the STA
                waits before timing out a TDLS setup request."
        DEFVAL { 18 }
::= { dot11StationConfigEntry 100 }

dot11TDLSProbeDelay OBJECT-TYPE
        SYNTAX INTEGER (1..65535)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute indicates the amount of time in units of microseconds the
                STA waits before transmitting on a new channel, in the absence of traffic on
                the channel that causes a CCA state to be created."
        DEFVAL { 1000 }
::= { dot11StationConfigEntry 101 }
```

Insert a new Annex U after Annex T:

Annex U (informative) Usage of Ethertype 89-0d

U.1 Ethertype 89-0d frame body

The Ethertype 89-0d frame body is specified in Figure U-1, omitting any possible security header and trailer.

	LLC	SNAP	Payload Type	Payload
Octets:	3	5	1	variable

Figure U-1—Ethertype 89-0d frame body

LLC is defined in ISO/IEC 8802-2:1998.

SNAP is defined in IEEE Std 802-2001. The formatting of the SNAP header is according to RFC 1042. The Ethertype is set to 89-0d.

The Payload Type field is set to one of the values in Table U-1.

Protocol Name	Payload Type	Subclause
Remote Request/Response	1	11A.10.3
TDLS	2	11.19.1
reserved	3-255	

Table U-1—Payload Type field values

The Payload depends on the value inside the Payload Type field, and is defined in the subclauses listed in Table U-1.