How to enable and verify TDLS function in Wi-Fi driver

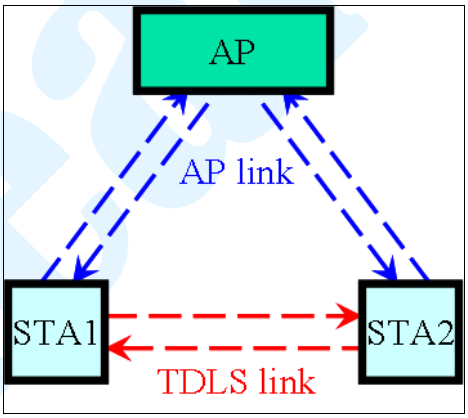
1. Brief introduction for TDLS

1.1 What is TDLS?

TDLS (Tunneled Direct Link Setup) is a Wi-Fi technology to transfer data and media faster between the devices that are already in the same wireless network, as the network architecture shown in the following figure.

The condition to setup a TDLS direct link between STA1 and STA2 is that both STAs has previously associated to the same AP. With the TDLS discovery and setup procedure between STA1 and STA2 via AP, the two STAs are able to establish a TDLS direct link, and the data traffic sent to each other can be delivered over the direct link, instead of over the AP, afterwards.

The TDLS technology is able to reduce the hop through the AP while transferring data between the two STAs, and thus yields higher throughput and lower latency, in comparison with the traditional Wi-Fi infrastructure mode.



1.2 The benefits of TDLS

- TDLS link can provide more efficient data transmission.
- TDLS link allows devices to perform the highest level of shared capabilities, regardless of the AP's capabilities.
- TDLS link supports WPA2 security, even if the network is using lower level of security.

2. Enable TDLS in Wi-Fi driver

2.1 Enable TDLS support from Makefile

/* turn on the flag of TDLS */

```
CONFIG_TDLS = y
```

/* use cfg80211 for I/O */

```
EXTRA_CFLAGS += -DCONFIG_IOCTL_CFG80211
-DRTW_USE_CFG80211_STA_EVENT
```

2.2 Re-build driver .ko file

```
# make
```

3. Setup TDLS direct link

As the TDLS setup initiator, the TDLS setup procedure can be performed on the DUT via wpa_cli commands, as the explanation below. **Both the DUT and the peer STA must associate to the same AP prior to the establishment of TDLS direct link, since the TDLS setup handshake needs to be executed based on the AP link.**

3.1 DUT associates to AP

In the following examples, we use "wlan0" as the target wlan device number. Users should replace it by the number corresponding to RTK wlan device on the test platform.

3.1.1 Setup and run wpa_supplicant

```
# cat wpa.conf
```

```
# cat p2p_supplicant.conf
ctrl_interface=/var/run/wpa_supplicant
update_config=1

# wpa_supplicant -Dnl80211 -i wlan0 -c ./wpa.conf &
```

3.1.2 Connect to AP

```
# wpa_cli –i wlan0 add_network
# wpa_cli –i wlan0 set_network 0 ssid '"AP_NONE"'
# wpa_cli –i wlan0 set_network 0 key_mgmt NONE
# wpa_cli –i wlan0 select_network 0
```

3.2 Initiates TDLS setup procedure

3.2.1 Initiate TDLS Setup

To initiate the TDLS setup procedure with the desired STA that has previously associated to the same AP.

/* # tdls_setup <addr> */
/* <addr> = MAC address of the desired STA to setup TDLS link */

```
# wpa_cli -i wlan0 tdls_setup 8c:3a:e3:41:3d:d7
```

3.2.2 Issue TDLS Teardown after test

To tear down the TDLS link with the TDLS peer STA.

/* # tdls_teardown <addr> */
/* <addr> = MAC address of the desired STA to tear down TDLS link */

```
# wpa_cli -i wlan0 tdls_teardown 8c:3a:e3:41:3d:d7
```

4. Verify the TDLS function

After the successful TDLS setup procedure between DUT and TDLS peer STA, the TDLS direct link should be established, and the data traffic sent to each other should be delivered over the direct link.

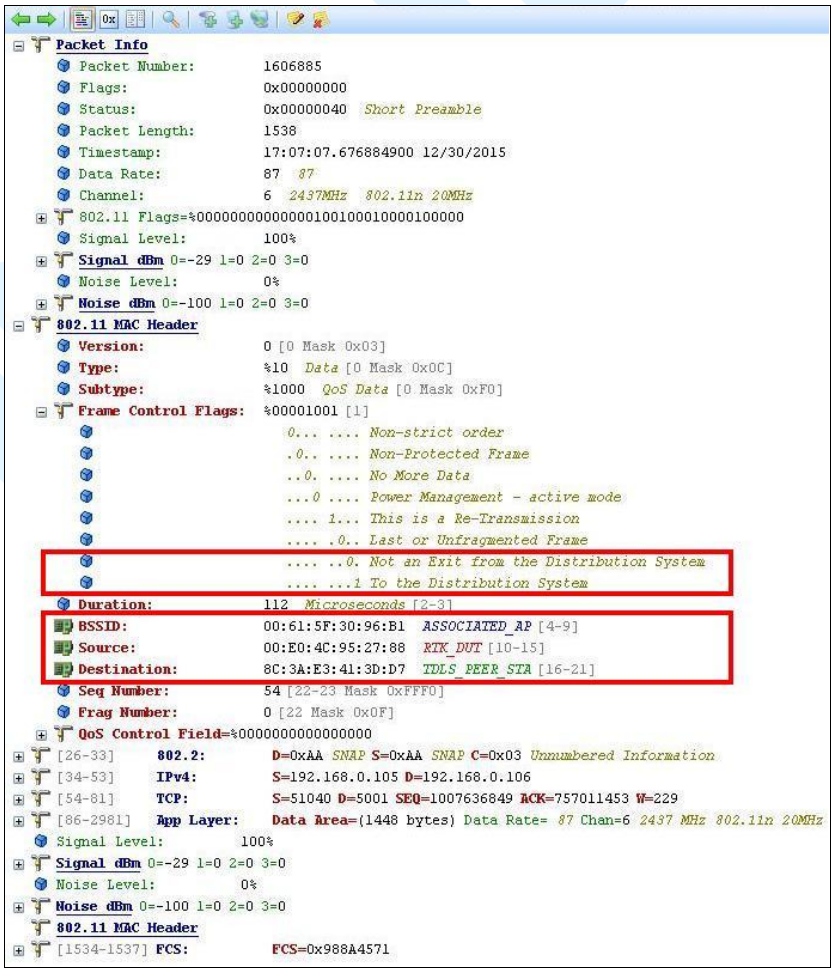
The behavior of data transmission over the TDLS direct link can be checked via observing the air sniffer or examining the dumped driver debug information.

In the following examples, "rtl8723cs" is the type of RTK wlan card. Users should replace it by the type name of RTK wlan device that is actually used on the test platform.

4.1 Before TDLS Setup

4.1.1 Observe from air sniffer

Before TDLS setup, the data frames sent from RTK DUT to TDLS peer STA are transferred over the AP link.



4.1.2 Observe from tdls_info under /proc entry

Before TDLS setup, only the information related to the associated AP is shown in tdls_info.

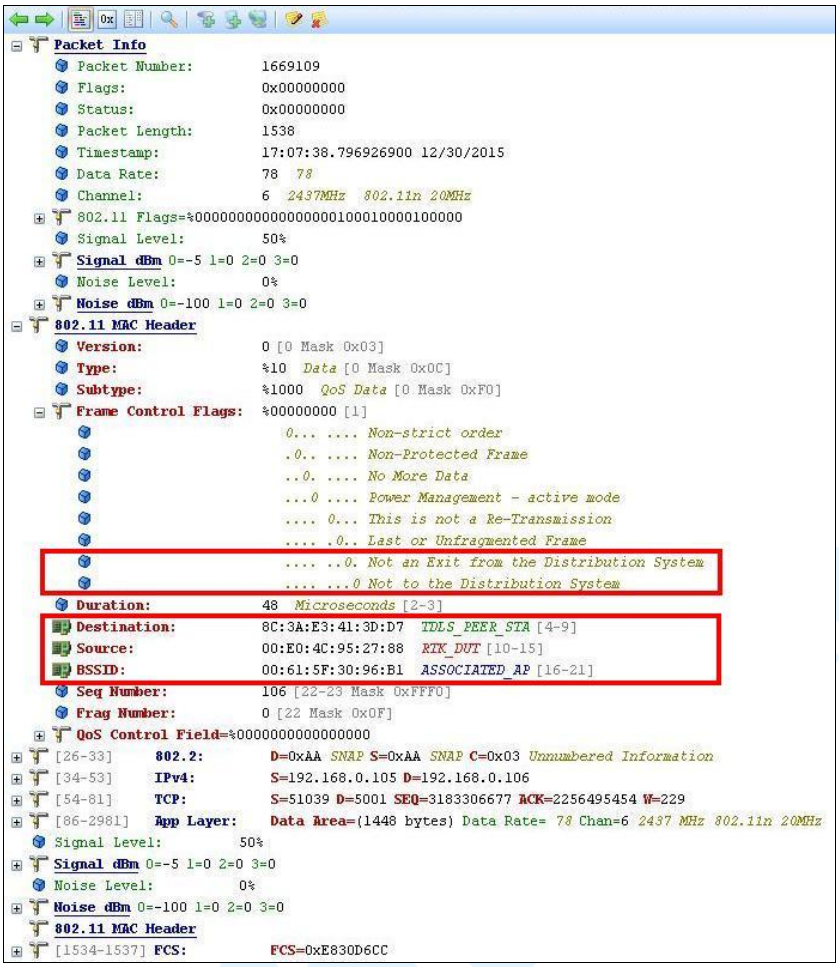
```
# cat /proc/net/rtl8723cs/wlan0/tdls_info


============[TDLS Function Info]============
TDLS Prohibited = _FALSE
TDLS Channel Switch Prohibited = _TRUE
TDLS Link Established = _FALSE
TDLS STA Num (Linked/Allowed) = 0/4
TDLS Allowed STA Num Reached = _FALSE
TDLS Device Discovered = _FALSE
TDLS Enable = _TRUE
TDLS Driver Setup = _TRUE
============[Associated AP/GO Info]============
BSSID = 615
Mac Address = 00:61:5f:30:96:b1
Wireless Mode = 11B 11G 11_24N
Privacy = NO PRIVACY
Channel = 6
Channel Offset = N/A
Bandwidth Mode = 20MHz
============[TDLS Peer STA Info]============
No TDLS direct link exists!
```

4.2 After TDLS Setup

4.2.1 Observe from air sniffer

After successful TDLS setup, the data frames sent from RTK DUT to TDLS peer STA are transferred over the TDLS direct link.



4.2.2 Observe from tdls_info under /proc entry

After successful TDLS setup, the information related to the TDLS peer STA will be displayed in tdls_info, including the Tx/Rx packet count that is transferred over the TDLS direct link.

```
# cat /proc/net/rtl8723cs/wlan0/tdls_info


============[TDLS Function Info]============
TDLS Prohibited = _FALSE
TDLS Channel Switch Prohibited = _TRUE
TDLS Link Established = _TRUE
TDLS STA Num (Linked/Allowed) = 1/4
TDLS Allowed STA Num Reached = _FALSE
TDLS Device Discovered = _TRUE
TDLS Enable = _TRUE
TDLS Driver Setup = _TRUE
```

==========[Associated AP/GO Info]==========

BSSID = 615

Mac Address = 00:61:5f:30:96:b1

Wireless Mode = 11B 11G 11_24N

Privacy = NO PRIVACY

Channel = 6

Channel Offset = N/A

Bandwidth Mode = 20MHz

==========[TDLS Peer STA Info: STA 1]==========

Mac Address = 8c:3a:e3:41:3d:d7

TDLS STA State = TDLS_RESPONDER_STATE

TDLS_LINKED_STATE

Wireless Mode = 11B 11G 11_24N

Bandwidth Mode = 20MHz

Privacy = NO PRIVACY

TPK Lifetime (Current/Expire) = 0 sec/1800 sec

Tx Packets Over Direct Link = 11292

Rx Packets Over Direct Link = 5196

root@fiber-3g:/ # cat /proc/net/rtl8723cs/wlan0/tdls_info

cat /proc/net/rtl8723cs/wlan0/tdls_info

==========[TDLS Function Info]==========

TDLS Prohibited = _FALSE

TDLS Channel Switch Prohibited = _TRUE

TDLS Link Established = _TRUE

TDLS STA Num (Linked/Allowed) = 1/4

TDLS Allowed STA Num Reached = _FALSE

TDLS Device Discovered = _TRUE

TDLS Enable = _TRUE

TDLS Driver Setup = _TRUE

==========[Associated AP/GO Info]==========

BSSID = 615

Mac Address = 00:61:5f:30:96:b1

Wireless Mode = 11B 11G 11_24N

Privacy = NO PRIVACY

Channel = 6

Channel Offset = N/A

Bandwidth Mode = 20MHz

==========[TDLS Peer STA Info: STA 1]==========

Mac Address = 8c:3a:e3:41:3d:d7
TDLS STA State = TDLS_RESPONDER_STATE
TDLS_LINKED_STATE
Wireless Mode = 11B 11G 11_24N
Bandwidth Mode = 20MHz
Privacy = NO PRIVACY
TPK Lifetime (Current/Expire) = 0 sec/1800 sec
Tx Packets Over Direct Link = 13882
Rx Packets Over Direct Link = 5196