Exploring capwap-discovery_ipv4_dhcp-opt43.pcapng

No IP	Broadcast	WLC C	WLC A	AP wired E	AP wired A

📁 **capwap-discovery_ipv4_dhcp-opt43.pcapng**

🔗 DHCP Discover

Transaction ID	0x000013c8
🌐 IP	0.0.0.0
Client MAC address	84:b2:61:0e:0c:18
Client MAC address	84:b2:61:0e:0c:18
🖥️ Hostname	AP84b2.610e.0c18

💡 DHCP — client obtains IP address after 802.11 association and EAPOL key exchange complete; DORA: Discover→Offer→Request→ACK; in WLAN, DHCP may traverse CAPWAP tunnel to WLC

🔗 DHCP Offer

Transaction ID	0x000013c8
🌐 IP	10.0.41.99
Client MAC address	84:b2:61:0e:0c:18

💡 DHCP — client obtains IP address after 802.11 association and EAPOL key exchange complete; DORA: Discover→Offer→Request→ACK; in WLAN, DHCP may traverse CAPWAP tunnel to WLC

🔗 DHCP Request

Transaction ID	0x000013c8
🌐 IP	0.0.0.0
Client MAC address	84:b2:61:0e:0c:18
Client MAC address	84:b2:61:0e:0c:18
🖥️ Hostname	AP84b2.610e.0c18

💡 DHCP — client obtains IP address after 802.11 association and EAPOL key exchange complete; DORA: Discover→Offer→Request→ACK; in WLAN, DHCP may traverse CAPWAP tunnel to WLC

🔗 DHCP ACK

Transaction ID	0x000013c8
🌐 IP	10.0.41.99
Client MAC address	84:b2:61:0e:0c:18

💡 DHCP — client obtains IP address after 802.11 association and EAPOL key exchange complete; DORA: Discover→Offer→Request→ACK; in WLAN, DHCP may traverse CAPWAP tunnel to WLC

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local
Type	A (1) (Host Address)

Frame 54 | 2017-01-14T12:47:31.193844Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local
Type	A (1) (Host Address)

Frame 56 | 2017-01-14T12:47:34.193452Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local
Type	A (1) (Host Address)

Frame 58 | 2017-01-14T12:47:37.193538Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local.lab.local
Type	A (1) (Host Address)

Frame 59 | 2017-01-14T12:47:40.193502Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local.lab.local
Type	A (1) (Host Address)

Frame 60 | 2017-01-14T12:47:43.193466Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local.lab.local
Type	A (1) (Host Address)

Frame 63 | 2017-01-14T12:47:46.19343Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local
Type	AAAA (28) (IP6 Address)

Frame 65 | 2017-01-14T12:47:49.193492Z

🔍 DNS Query

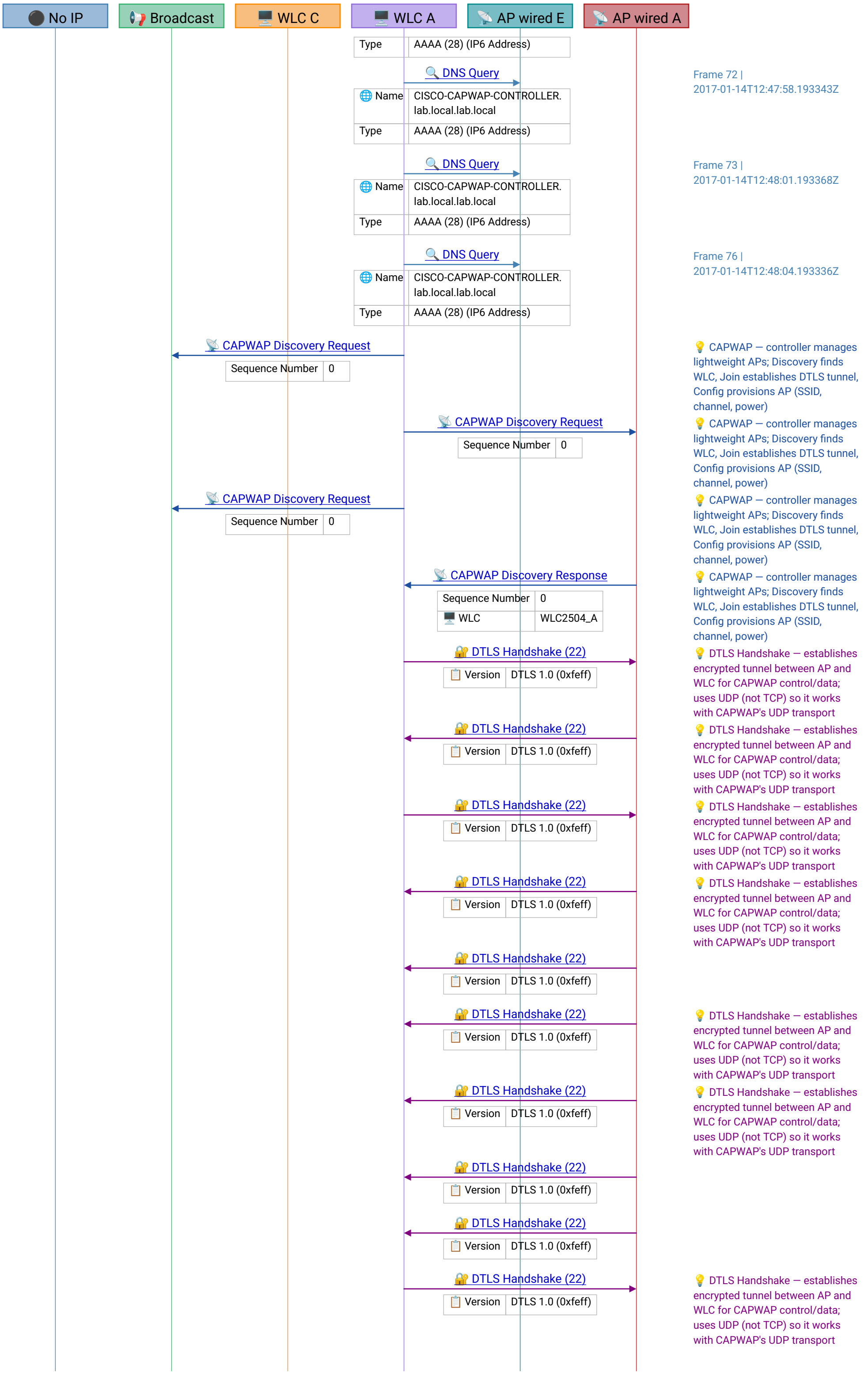
🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local
Type	AAAA (28) (IP6 Address)

Frame 66 | 2017-01-14T12:47:52.19336Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER.lab.local

Frame 69 | 2017-01-14T12:47:55.193241Z


No IP
Broadcast
WLC C
WLC A
AP wired E
AP wired A
Type
AAAA (28) (IP6 Address)
DNS Query
Name
CISCO-CAPWAP-CONTROLLER.lab.local.lab.local
Type
AAAA (28) (IP6 Address)
Frame 72 | 2017-01-14T12:47:58.193343Z
DNS Query
Name
CISCO-CAPWAP-CONTROLLER.lab.local.lab.local
Type
AAAA (28) (IP6 Address)
Frame 73 | 2017-01-14T12:48:01.193368Z
DNS Query
Name
CISCO-CAPWAP-CONTROLLER.lab.local.lab.local
Type
AAAA (28) (IP6 Address)
Frame 76 | 2017-01-14T12:48:04.193336Z
CAPWAP Discovery Request
Sequence Number
0
CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)
CAPWAP Discovery Request
Sequence Number
0
CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)
CAPWAP Discovery Request
Sequence Number
0
CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)
CAPWAP Discovery Response
Sequence Number
0
WLC
WLC2504_A
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS Handshake (22)
Version
DTLS 1.0 (0xfeff)
DTLS — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

Exploring capwap-discovery_ipv4_dhcp-opt43.pcapng

⚫ No IP | 📢 Broadcast | 🖥️ WLC C | 🖥️ WLC A | 📡 AP wired E | 📡 AP wired A

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔒 DTLS Change Cipher Spec (20)

Frame 95 | 2017-01-14T12:48:17.490324Z

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)
📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔒 DTLS Application Data (23)

📋 Version	DTLS 1.0 (0xfeff)
🔢 Epoch	1
📦 Length	1440

Frame 98 | 2017-01-14T12:48:17.608339Z

🔒 DTLS Application Data (23)

📋 Version	DTLS 1.0 (0xfeff)
🔢 Epoch	1
📦 Length	1440

Frame 99 | 2017-01-14T12:48:17.609815Z

⚠️ DTLS Alert (21)

Frame 105 | 2017-01-14T12:48:18.843664Z

📡 CAPWAP Discovery Request

Sequence Number	0

💡 CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)

📡 CAPWAP Discovery Request

Sequence Number	0

💡 CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)

📡 CAPWAP Discovery Request

Sequence Number	0

💡 CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)

⚠️ DTLS Alert (21)

Frame 112 | 2017-01-14T12:48:20.067681Z

📋 ICMP Type 3

Code	3 (Port unreachable)

Frame 113 | 2017-01-14T12:48:20.06781Z

📡 CAPWAP Discovery Response

Sequence Number	0
🖥️ WLC	WLC2504_A

💡 CAPWAP — controller manages lightweight APs; Discovery finds WLC, Join establishes DTLS tunnel, Config provisions AP (SSID, channel, power)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data;

⚫ No IP | 📢 Broadcast | 🖥️ WLC C | 🖥️ WLC A | 📡 AP wired E | 📡 AP wired A

📋 Version	DTLS 1.0 (0xfeff)

uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔒 DTLS Change Cipher Spec (20)

Frame 129 | 2017-01-14T12:48:30.3603Z

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)
📋 Version	DTLS 1.0 (0xfeff)

💡 DTLS Handshake — establishes encrypted tunnel between AP and WLC for CAPWAP control/data; uses UDP (not TCP) so it works with CAPWAP's UDP transport

🔒 DTLS Application Data (23)

📋 Version	DTLS 1.0 (0xfeff)
🔢 Epoch	1
📦 Length	1440

Frame 132 | 2017-01-14T12:48:30.474713Z

🔒 DTLS Application Data (23)

📋 Version	DTLS 1.0 (0xfeff)
🔢 Epoch	1
📦 Length	1440

Frame 133 | 2017-01-14T12:48:30.476305Z