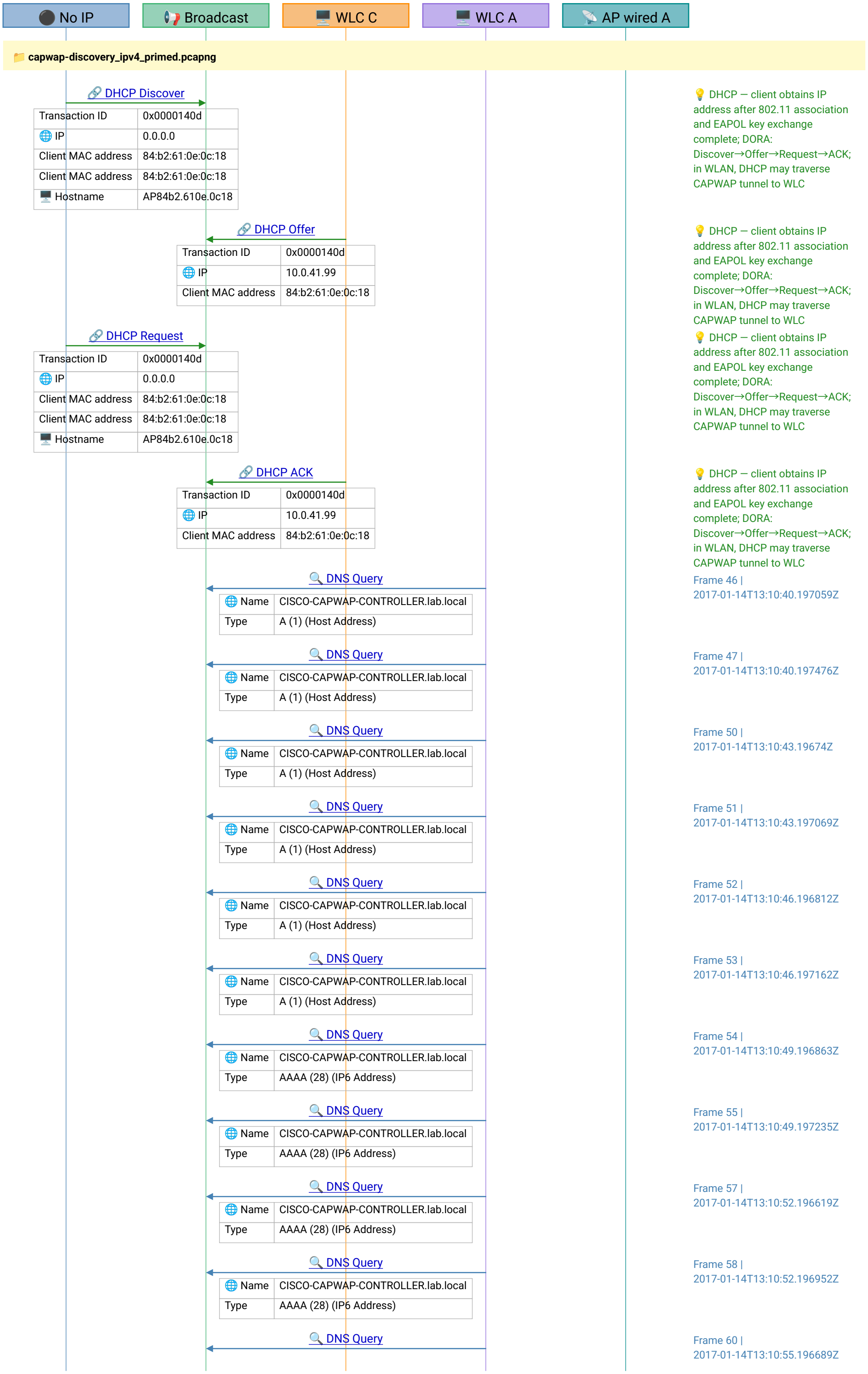

No IP
Broadcast
WLC C
WLC A
AP wired A
capwap-discovery_ipv4_primed.pcapng
DHCP Discover
Transaction ID 0x0000140d
IP 0.0.0.0
Client MAC address 84:b2:61:0e:0c:18
Client MAC address 84:b2:61:0e:0c:18
Hostname AP84b2.610e.0c18
DHCP — client obtains IP address after 802.11 association and EAPOL key exchange complete; DORA: Discover→Offer→Request→ACK; in WLAN, DHCP may traverse CAPWAP tunnel to WLC
DHCP Offer
Transaction ID 0x0000140d
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 0x0000140d
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 0x0000140d
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
Frame 46 | 2017-01-14T13:10:40.197059Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type A (1) (Host Address)
Frame 47 | 2017-01-14T13:10:40.197476Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type A (1) (Host Address)
Frame 50 | 2017-01-14T13:10:43.19674Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type A (1) (Host Address)
Frame 51 | 2017-01-14T13:10:43.197069Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type A (1) (Host Address)
Frame 52 | 2017-01-14T13:10:46.196812Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type A (1) (Host Address)
Frame 53 | 2017-01-14T13:10:46.197162Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type AAAA (28) (IP6 Address)
Frame 54 | 2017-01-14T13:10:49.196863Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type AAAA (28) (IP6 Address)
Frame 55 | 2017-01-14T13:10:49.197235Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type AAAA (28) (IP6 Address)
Frame 57 | 2017-01-14T13:10:52.196619Z
DNS Query
Name CISCO-CAPWAP-CONTROLLER.lab.local
Type AAAA (28) (IP6 Address)
Frame 58 | 2017-01-14T13:10:52.196952Z
DNS Query
Frame 60 | 2017-01-14T13:10:55.196689Z

Exploring capwap-discovery_ipv4_primed.pcapng

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

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

🔍 DNS Query

Frame 61 | 2017-01-14T13:10:55.197019Z

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

📡 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 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

💡 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

💡 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

💡 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

💡 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)

📋 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 — 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)

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

🔐 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 85 | 2017-01-14T13:11:08.492884Z

🔐 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 88 | 2017-01-14T13:11:08.604239Z

🔒 DTLS Application Data (23)

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

Frame 89 | 2017-01-14T13:11:08.605981Z

⚠️ DTLS Alert (21)

Frame 96 | 2017-01-14T13:11:10.342523Z

📡 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 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 104 | 2017-01-14T13:11:11.04795Z

📋 ICMP Type 3

Code	3 (Port unreachable)

Frame 105 | 2017-01-14T13:11:11.048437Z

📡 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)

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

📡 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)

📡 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)

📋 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 — 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 123 | 2017-01-14T13:11:21.34045Z

🔐 DTLS Handshake (22)

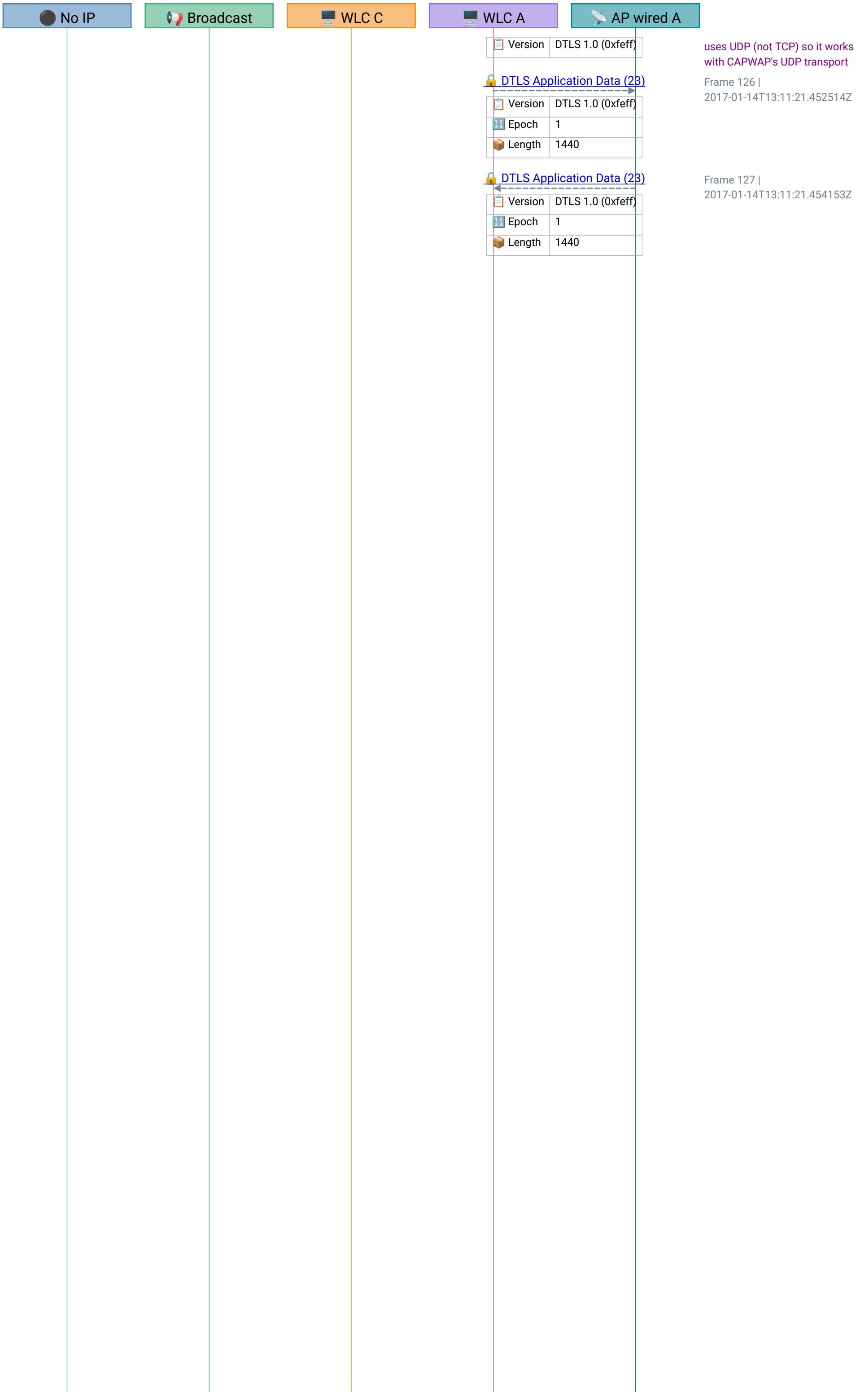
📋 Version	DTLS 1.0 (0xfeff)

💡 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;


No IP
Broadcast
WLC C
WLC A
AP wired A
Version
DTLS 1.0 (0xfeff)
uses UDP (not TCP) so it works with CAPWAP's UDP transport
DTLS Application Data (23)
Frame 126 | 2017-01-14T13:11:21.452514Z
Version
DTLS 1.0 (0xfeff)
Epoch
1
Length
1440
DTLS Application Data (23)
Frame 127 | 2017-01-14T13:11:21.454153Z
Version
DTLS 1.0 (0xfeff)
Epoch
1
Length
1440