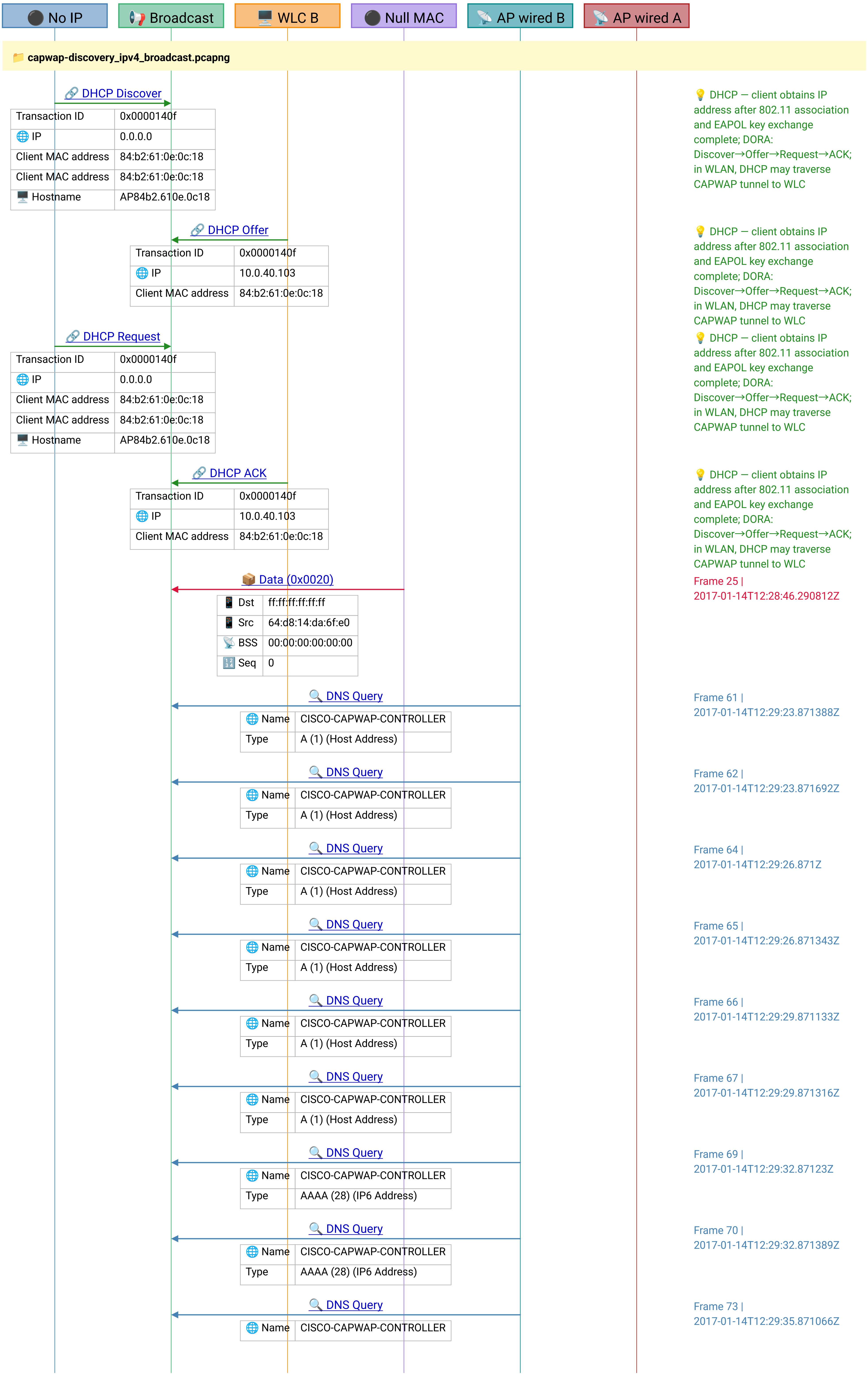
Exploring capwap-discovery_ipv4_broadcast.pcapng



📁 **capwap-discovery_ipv4_broadcast.pcapng**

🔗 DHCP Discover

Transaction ID	0x0000140f
🌐 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	0x0000140f
🌐 IP	10.0.40.103
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	0x0000140f
🌐 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	0x0000140f
🌐 IP	10.0.40.103
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

📦 Data (0x0020)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	64:d8:14:da:6f:e0
📡 BSS	00:00:00:00:00:00
🔢 Seq	0

Frame 25 | 2017-01-14T12:28:46.290812Z

🔍 DNS Query

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

Frame 61 | 2017-01-14T12:29:23.871388Z

🔍 DNS Query

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

Frame 62 | 2017-01-14T12:29:23.871692Z

🔍 DNS Query

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

Frame 64 | 2017-01-14T12:29:26.871Z

🔍 DNS Query

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

Frame 65 | 2017-01-14T12:29:26.871343Z

🔍 DNS Query

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

Frame 66 | 2017-01-14T12:29:29.871133Z

🔍 DNS Query

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

Frame 67 | 2017-01-14T12:29:29.871316Z

🔍 DNS Query

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

Frame 69 | 2017-01-14T12:29:32.87123Z

🔍 DNS Query

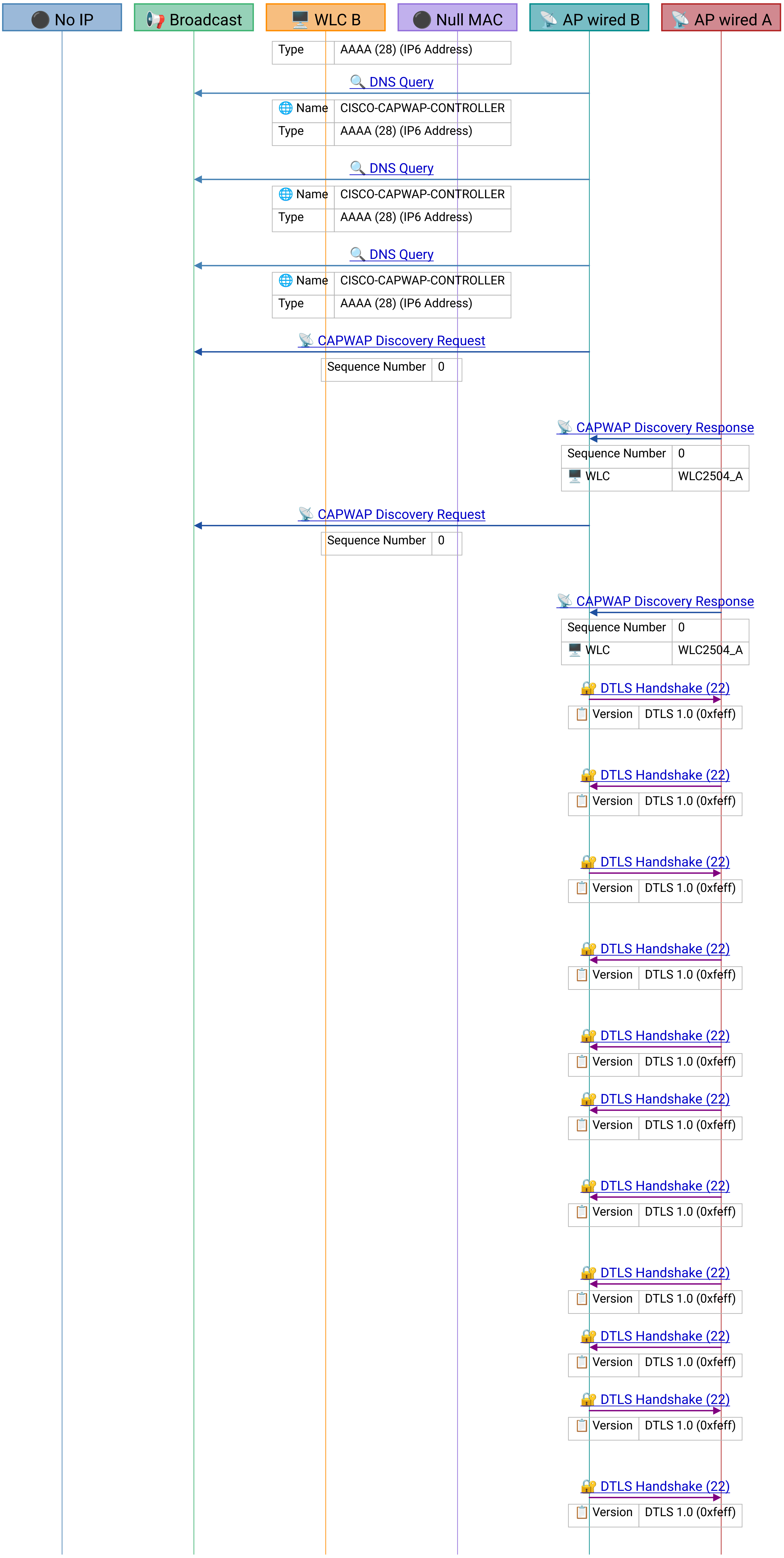
🌐 Name	CISCO-CAPWAP-CONTROLLER
Type	AAAA (28) (IP6 Address)

Frame 70 | 2017-01-14T12:29:32.871389Z

🔍 DNS Query

🌐 Name	CISCO-CAPWAP-CONTROLLER

Frame 73 | 2017-01-14T12:29:35.871066Z



Type	AAAA (28) (IP6 Address)

🔍 DNS Query

Frame 74 | 2017-01-14T12:29:35.87122Z

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

🔍 DNS Query

Frame 75 | 2017-01-14T12:29:38.870949Z

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

🔍 DNS Query

Frame 76 | 2017-01-14T12:29:38.871288Z

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

📡 CAPWAP Discovery Request

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

Sequence Number	0

📡 CAPWAP Discovery Response

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

Sequence Number	0
🖥️ WLC	WLC2504_A

📡 CAPWAP Discovery Request

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

Sequence Number	0

📡 CAPWAP Discovery Response

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

Sequence Number	0
🖥️ WLC	WLC2504_A

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

💡 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

📋 Version	DTLS 1.0 (0xfeff)

🔐 DTLS Handshake (22)

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

📋 Version	DTLS 1.0 (0xfeff)

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 99 | 2017-01-14T12:29:53.167379Z

🔐 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 103 | 2017-01-14T12:29:53.30007Z

🔒 DTLS Application Data (23)

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

Frame 104 | 2017-01-14T12:29:53.301274Z