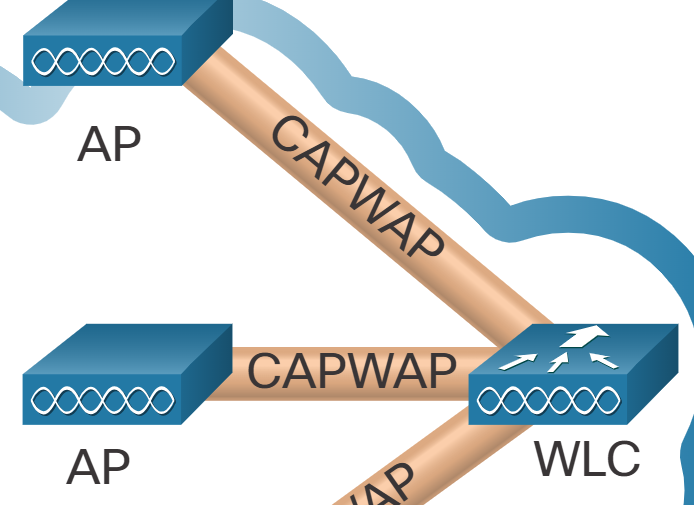
CAPWAP (Control and Provisioning of Wireless Access Points) - Điều Khiển và Cung Cấp Điểm Truy Cập Không Dây



**I. Split MAC Address**

A screenshot of a computer program

AI-generated content may be incorrect. **II. DTLS (Datagram Transport Layer Security)**

* Purpose: Secure datagram-based applications (UDP).
* Foundation: Based on TLS, adapted for datagram environments.
* Functions:
  + Encryption: Protects data confidentiality.
  + Authentication: Verifies communication partners.
  + Integrity: Ensures data hasn't been altered.
* Operation:
  + Uses symmetric and asymmetric encryption.
  + Employs digital certificates for authentication.
  + Utilizes Message Authentication Codes (MACs) for data integrity.
  + Handles packet loss, reordering, and duplication (UDP characteristics).
* Key Components:
  + Record Protocol: Encapsulates application data, provides security.
  + Handshake Protocol: Establishes secure connection.
  + Alert Protocol: Communicates errors and warnings.
* Benefits:
  + Secures UDP-based applications (VoIP, video, gaming).
  + TLS compatibility for security algorithms.
  + Designed for datagram communication.
* Applications:
  + VoIP and video streaming.
  + Online gaming.
  + CAPWAP.
  + UDP-based VPNs.

1. CAPWAP can operate either over IPv4 or IPv6, but uses IPv4 by default.  
2. CAPWAP for **IPv4 uses IP protocol 17 in the frame header and UDP ports 5246 and 5247.**3. CAPWAP for **IPv6 uses IP protocol 136 in the frame header and UDP ports 5246 and 5247.**4. The AP is responsible for the following in the split MAC architecture for CAPWAP:  
\* Beacons and probe responses  
\* Packet acknowledgments and retransmissions  
\* Frame queueing and packet prioritization  
\* MAC layer data encryption and decryption  
5. The WLC is responsible for the following in the split MAC architecture for CAPWAP:  
\* Authentication  
\* Association and re-association of roaming clients  
\* Frame translation to other protocols  
\* Termination of 802.11 traffic on a wired interface  
6. The correct answer is False: DTLS must be configured on the CAPWAP data tunnels, but is enabled by default on the CAPWAP control tunnel.  
7. A FlexConnect AP can operate in the following modes:  
\* In connect mode, the WLC is reachable and performs all its CAPWAP functions.  
\* In standalone mode, the WLC is unreachable and the AP switches local traffic and performs client authentication locally.