

AP HW Passed DOA Validation

CAPWAP

- DHCP Option 43**
 - Make Sure the Option 43 is enabled on the DHCP Server
 - If you are using Vendor Specific Options(60) on DHCP then make sure the right VCI Strings are configured on DHCP server
 - Always Try to use HEX value while configuring Option 43 on DHCP server
 - Option 43 example
 - WLC 1 - 192.168.10.5 (Hex Value- c0a80a05)
 - WLC 2 - 192.168.10.20 (Hex Value- c0a80a14)
 - Type - '0x1'
 - Length is 2 * 4 = 8 = '0x08'
 - Hex Value for Option 43 = 'f108c0a80a05c0a80a14' (Incase of only one WLC the starting four characters will change to 'f104')
 - IOS command = 'option 43 hex f108c0a80a05c0a80a14'
- DNS**
 - Make Sure the is a Valid DNS server is available in the Network
 - Make Sure the WLC IP entries are added in to the DNS server (CISCO-CAPWAP-CONTROLLER.localdomain/CISCO-LWAPP-CONTROLLER.localdomain)
 - Make Sure the DNS server IP details are getting shared by DHCP server to the AP
 - Make Sure the DNS (Port 53) communication is not blocked on Firewall/ACLs in the network
- Discovery**
 - This option is applicable only after the First Successful association of the AP to any one of the WLC
- Stored WLC information**
 - AP will store the WLC information in Local NVRAM after the first successful association
 - In Case of AP Priming is in use APs will try to associate to the WLC based on the Primary Secondary and Tertiary controller preferences
 - APs also keeps the Mobility Members address of the WLC that AP successfully joined
 - Sub Topic
- IP Helper Address**
 - Make Sure the AP VLAN Gateway is configured right WLC IP as a Helper Address for using this Discovery Model
 - Configuration Example
 - ip helper-address x.x.x.x -> WLC Management IP
 - ip forward protocol udp 12222 (For OLD or RCV Image APs)
 - ip forward protocol udp 12223 (For OLD or RCV Image APs)
 - ip forward-protocol udp 5246
 - ip forward-protocol udp 5247
- UDP Ports**
 - Make Sure the UDP Ports 5246 and 5247 are allowed in the network - CAPWAP
 - Make Sure the UDP Ports 12222 and 12223 are allowed in the network - LWAPP
- Path MTU**
 - CAPWAP-Dynamic P-MTU Discovery - AP starts from the lowest MTU (576) and increases every 30 seconds in steps of (576, 1006, 1492, 1500)
 - Jumbo Frames are not supported on Cisco AP
 - 1499 Bytes = Ethernet + CAPWAP PMTU
 - CAPWAP PMTU = Outer IP + UDP + DTLS
 - Ethernet = 14 Bytes
 - CAPWAP PMTU = 1485 Bytes
 - Outer IP = 20 Bytes
 - UDP = 25 Bytes
 - DTLS = 1440 Bytes
 - Always Try to avoid a Fragmentation happening for CAPWAP Control Traffic
 - For Better results try to provide fragmentation and reassembly at the application layer using the Right MTU

Cable

- Connected**
 - Yes
 - No - Connect Cable
- Length**
 - Solid-Strand - UP-TO 90m
 - Multi-Strand - UP-TO 10m
 - Total 100m
- Type**
 - Cat5 - 100MHz - 10/100Mbps - POE up-to 15.4w
 - Cat5e - 100MHz - 10/100/1000Mbps - POE+ up-to 30w
 - Cat6 - 250MHz - 10/100Mbps, 1-10Gbps
- Connection Status**
 - Check the Cable and replace found faulty
 - Use cable-diagnostics feature on Cisco Switches for cabling issues
- Switch Port Status**
 - Speed - Make sure the speed is negotiated correctly on both sides
 - Duplex - Make sure the Duplex is negotiated correctly on both sides
 - Type - Make sure the port type is detected correctly on both devices
 - STP - Make sure the STP is not blocking any of the ports connected to WLC
 - errDisable - Make sure the Switch Port is not in errDisable state due any error conditions
- Switch Port Security**
 - 802.1x - Make sure the 802.1x Credentials are provided to the AP
 - If you are connecting the Factory Default/New AP then 802.1x needs to be disabled for the first WLC Association
 - MAC - Make sure the AP MAC is allowed on the Switch Port
 - Make sure the No of MAC address permitted on the Port is matching the requirements

POE

- Switch Power Supply**
 - Make sure the POE Switch is using right power supply based on No of APs and the POE requirement choose the right power supply for the switch.
 - Make sure POE switch is having sufficient remaining Power to support the new APs. Try to keep the power utilization less than 80% of the available power
- Power Injector**
 - Make sure the we are using the compatible Power Injector as per the AP Data sheet
- POE/802.af**
 - POE Supported Switch - Make sure we are connecting only the APs that can run on 15.4w power
- POE+/802.at**
 - POE+ Supported Switch
 - Make sure we are using the right cable for supporting the POE+ requirements
 - Make sure the distance is matching the power requirements
 - Make sure CDP/LLDP is running for POE Power negotiation

Regulatory domain

- Country**
 - Make sure the countries are added on WLC as the list of sites getting served by the WLC
 - Make sure the APs getting connected to the WLC is as per the country regulatory domain

License

- AP License**
 - Make sure the WLC is having sufficient AP licenses to support the no of APs getting added
 - Make sure the right license is in active state
 - Make sure the HA WLC have sufficient licenses in the case of N+1/N+N scenarios
 - Make sure the system time is valid in case of Evaluation License

Certificate

- MIC**
 - Make Sure the Certificate Time is Valid and Not expired
 - Make Sure the MIC Certificate is Accepted by the WLC in the AP Policies
- LSC**
 - Make Sure the Certificate Time is Valid and Not expired
 - Make Sure the MIC Certificate is Accepted by the WLC in the AP Policies
 - Make Sure the AP is installed with the right LSC certificate as per the Cert Server in the Network
- SSC**
 - Make Sure the Certificate Time is Valid and Not expired
 - Make Sure the MIC Certificate is Accepted by the WLC in the AP Policies
 - Make Sure the AP is installed with the right SSC certificate

Layer 3 Connectivity

- APs are able to Communicate to the AP VLAN Gateway**
 - Make Sure the AP is configured with a valid IP address based on the Network IP Schema
 - Make sure the AP interface and the Switch Port VLAN are configured as per Design
 - Make sure the AP VLAN is available on the Switch VLAN Database
 - Make sure the AP VLAN is available in the Allowed VLAN list of the connected Switch port
 - Make sure the AP VLAN is available in the VLAN Database and Allowed VLAN list of the UPLINK Switch ports of the Intermediate Switches
 - Make sure there is no Duplicate IP scenario exists in the network for the IP configured on the AP
- APs are able to communicate to the WLC Management IP**
 - Use Extended Ping from the GW SW with source as the VLAN interface or Trace Route to find the Drop location and Fix the Routing Issues
 - Make sure GW Switch is having the route to access the External network
 - Make sure the AP VLAN route is available in the Routing Table for all Intermediate Routers
 - Make sure there is no Fire Wall blocking the traffic from AP VLANs
 - Make sure there is no ACL blocking the traffic from AP VLANs
- Incase of Nated AP Management on WLC make sure APs are able to communicate to the Natted Interface of the WLC
- Make Sure APs are able to communicate to the Dedicated AP Manager Interface for the AP Dynamic Management if any

IP Address

- DHCP**
 - Make Sure the APs are connected to the right switch port with the right VLAN
 - Make Sure the AP VLAN have the reachability to the DHCP Server
 - Make Sure the Current Helper Address is configured on the AP VLAN Gateway Switch
 - Make Sure there is a Valid IP Pool is available for AP VLAN
 - Make Sure there are Required Number for Free IP Address are available based on the No of APs in the Network
 - Make Sure there is no Duplicate IP Scenario for the IP used on AP
 - Make Sure the DHCP server is able to serve the Clients, Restart the DHCP service if Required
- Static**
 - Make Sure the right IP and Subnet Mask is configured on the AP
 - Make Sure the Switch Port is configured correctly with the Right Switch Port Mode accessibility
 - Make Sure the Gateway is configured and AP is able to communicate to the Gateway Switch
 - Make Sure there is no Duplicate IP Scenario for the IP used on AP
- AP Mode**
 - Local - Make Sure the Switch port is configured with Access VLAN or Native VLAN on Trunk Port
 - Flex Connect - Make Sure the Switch Port is configured for the Right Native VLAN is the Native VLAN support is enabled on the AP
 - Make Sure the Native VLAN on the Switch Is not getting Tagged from Switch side while using the Native VLAN support is enabled on the Flex-Connect AP

Mesh AP

- Make sure all CAPWAP Discovery issues mentioned before are checked
- Make Sure the MESH AP Mac address is updated MAC Filter List of the WLC for the RAPs
- Make sure the MAP MAC Address is updated in the AP Authentication Policies
- Make Sure you are setting the MESH AP ROLE on the controller
- Make sure the Radius Configurations are correct if you are using Radius Authentication for MESH APs
- Make Sure the PSK Keys are configured currently on WLC and The MAPs in the PSK Provisioning is enabled for the Mesh APs
- Make Sure the "Default PSK" option is enabled in-case of using this feature for MESH AP Provisioning
- Make Sure there is no RF Signal Related issued between MESH APs, Radio/Antenna Settings should be valid for ALL Mesh APs

WLC Code

- Make Sure the WLC is Running the CODE that supports the AP model in use
- Make Sure the AP Image Bundle is also upgraded in case of 5508 with new throttles