Troubleshooting IoT Services: Controller

Reprovisioning IoT Services After Failover

What settings are needed to allow access via NETCONF?

To enable access via the Network Configuration Protocol (NETCONF), configure the following settings on your wireless controller:

1. Enable the authentication, authorization, and accounting (AAA) new model by entering the following command in the global configuration mode:

   ```
   aaa new-model
   ```

2. Set the default AAA authentication for login to the local user database with the command:

```
aaa authentication login default local
```

3. Specify the default AAA authorization for exec (shell access) to use the local user database by using the command:

```
aaa authorization exec default local
```

Enter these commands in the global configuration mode of your wireless controller:

```
wireless controller# configure terminal
wireless controller(config)# aaa new-model
wireless controller(config)# aaa authentication login default local
wireless controller(config)# aaa authorization exec default local
```

After executing these commands, your wireless controller should be properly configured to allow access through NETCONF using the local user database for authentication and authorization.

The global configuration for BLE radio has to be enabled on Wireless Controller. How do I verify the setting?

This task shows you how to verify if you have enabled BLE radio on the wireless controller at a global configuration level. This is a necessary setting.

Run the command: **show running-config | include ap dot15**

```
wireless controller# show running-config | include ap dot15
no ap dot15 shutdown
```

Verify if the output is `no ap dot15 shutdown`. This output indicates that the dot15 BLE radios are not shut down.

For the gRPC connection to work, a streaming token is required on the Wireless Controller. How do I view the token?

To establish a functioning gRPC connection, a gRPC streaming token must be present on the wireless controller. To verify the token, execute the **show running-config | include ap cisco-dna** command on the command on the wireless controller

```
wireless-controller# show running-config | include ap cisco-dna

ap cisco-dna token 0 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOjE2MjUs
ImNpZCI6Mzc4NTc3ODI1NDI2NzIyNjUwMDAsImVwIjoiMTAuMzAuMTE0LjEwODo4MDAwIiwiaW
F0IjoxNTg1NzA2OTIxfQ.56vXfL1IGrss6TJZDQaWVarAoTWZsIhbe3tGVMEJNYk
```

The resulting output will display the gRPC streaming token. For example:

```
ap cisco-dna token 0 <token_string>
```

Ensure that this token corresponds with the token configured on the access point (AP). You can check the AP's token by running the **show cloud connector key authentication** command.

Additionally, to examine the encoded information contained in the token, you can input the token into a JWT decoder like the one found at http://jwt.io/. Here is an example of the kind of payload data you might see:

```
PAYLOAD:DATA
{
  "tid": 1625,
  "cid": 37857782542672265000,
  "ep": "10.30.114.108:8000",
  "iat": 1585706921
}
```

gRPC must be enabled in the access point join profile. How do I verify the join profile has gRPC enabled?

This procedure demonstrates how to enable gRPC in the AP join profile, a necessary configuration.

To view the active settings, run the **show running-config | begin ap profile default-ap-profile** command.

```
controller# show running-config | begin ap profile default-ap-profileap profile
default-ap-profile
 apphost
 cisco-dna grpc
 description "default ap profile"
 mgmtuser username admin password 0 Cisco123! secret 0 Cisco123!
 ssh
trapflags ap crash
trapflags ap noradiocards
trapflags ap register
netconf-yang
end
```

This output reveals the configuration for the default AP profile. Should you require a different profile, apply the command accordingly, replacing **`default-ap-profile`** with the desired profile name.

Ensure the configuration includes the line `cisco-dna grpc`. This line confirms that gRPC is enabled for all access points utilizing this profile.

How do I verify gRPC is up?

To verify whether gRPC is operational, execute the **show ap grpc summary** command.

This command displays the gRPC connection status for each AP connected to the wireless controller, as shown in the example below:

```
controller# show ap grpc summary
AP Name                          AP Mac               gRPC Status
-------------------------------------------------------------------------------------
AP_10.2830                       04eb.409f.a7e0       Up
AP_02.2898                       04eb.409f.ab20       Up
AP_06.28CC                       04eb.409f.acc0       Up
AP_08.28E0                       04eb.409f.ad60       Up
AP_07.28E4                       04eb.409f.ad80       Up
AP_09.28EC                       04eb.409f.adc0       Up
AP_01.28F0                       04eb.409f.ade0       Up
AP_03.2928                       04eb.409f.afa0       Up
AP_05.2934                       04eb.409f.b000       Up
AP_04.2938                       04eb.409f.b020       Up
```

Each AP's name, MAC address, and gRPC status are listed. A status of `Up` indicates that gRPC is active and running for that AP.

.

How do I verify that TDL subscriptions are created and are valid?

1. To initiate the process of viewing all current telemetry subscriptions and to check their types and validity statuses, input the command below:

   ```
   show telemetry ietf subscription all
   ```

2. After executing the command, the wireless controller presenst a summarized output of the telemetry subscriptions. Enterprise Data Management (EDM) configures six distinct subscriptions, which you can identify by their numbers ranging from 122 to 127.

   Here is a sample of what the command's output might look like:

   ```
   wireless controller# show telemetry ietf subscription all
   Telemetry subscription brief
   ID     Type          State    Filter type
   ----------------------------------------
   122    Configured    Valid    tdl-uri
   123    Configured    Valid    tdl-uri
   124    Configured    Valid    tdl-uri
   125    Configured    Valid    transform-name
   126    Configured    Valid    transform-name
   ```

The output enumerates each subscription's unique ID, its configuration status, the validity of the state, and the applied filter type.

Are the TDL subscriptions created and valid?

Run the command **show telemetry ietf subscription all** command on the wireless controller.

The command displays the subscriptions, the subscription type, and if a subscription is valid. IoT Service creates five different subscriptions 122-126.

```
wireless controller# show telemetry ietf subscription all
  Telemetry subscription brief

  ID               Type        State       Filter type
  -------------------------------------------------------
  122              Configured  Valid       tdl-uri
  123              Configured  Valid       tdl-uri
  124              Configured  Valid       tdl-uri
  125              Configured  Valid       transform-name
  126              Configured  Valid       transform-name
```

What is the TDL status?

Execute the **show telemetry ietf subscription ID receiver** command on the wireless controller.

The command presents the status of Telemetry Description Language (TDL) subscriptions.

```
wireless controller# show telemetry ietf subscription 125 receiver
Telemetry subscription receivers detail:

  Subscription ID: 125
  Address: 10.22.243.33
  Port: 8004
  Protocol: cloud-native
  Profile:
  Connection: 33
  State: Connected
  Explanation:
```

The IoT Service manages five distinct subscriptions, with IDs from 122 to 126. For each subscription:

- Verify that the **Address** matches the IP address of the Cisco Spaces: Connector.
- Confirm that the **State** is **Connected**

  .

How do I view the current CAPWAP values for an AP?

1. Enter the command without any dots in the MAC address of the AP:

   `test platform software database get ewlc_oper/capwap_data;wtp_mac=`*`mac_without_dots`*

For example:

```
wireless controller# test platform software database get
ewlc_oper/capwap_data;wtp_mac=1cd1e065c340
```

The output presents a table with various records:

- Index 0 contains the AP's MAC address, IP address, model, and other static information.
- The **`device_detail.static_info`** section includes the AP's model, memory type, CPU type, and memory size, among other details.
- The **`device_detail.wtp_version section`** includes backup software version, mini iOS version, hardware version, and the current software version that the AP is running.
- The **`ap_services`** section gives details about monitor mode, DHCP server status, and sniffer interface ID.
- The **`tag_info`** section indicates whether the AP has any misconfigured tags.
- The **`external_module_data`** section displays information about any external modules connected to the AP, including product ID and version.
- The **`ap_state`** section displays administrative and operational states of the AP.
- The **`ap_mode_data`** section details the current mode and sub-mode of the AP.

```
wireless-controller# test platform software database get
ewlc_oper/capwap_data;wtp_mac=1cd1e065c340
Table Record Index 0 = {
 [0] wtp_mac = 1CD1.E065.C340
 [1] ip_addr = 10.22.243.229
 [2] name = AP84F1.47B2.B868
 [3] device_detail.static_info.board_data.model = C9115AXI-B
 [4] device_detail.static_info.board_data.wtp_serial_num = FJC25331LCY
```

```
 [5] device_detail.static_info.board_data.card_id = 0
 [6] device_detail.static_info.board_data.card_rev = 0
 [7] device_detail.static_info.board_data.wtp_enet_mac = 84F1.47B2.B868
 [8] device_detail.static_info.board_data.ap_sys_info.mem_type = DDR3
 [9] device_detail.static_info.board_data.ap_sys_info.cpu_type =  ARMv8 Processor rev 0
(v8l)
 [10] device_detail.static_info.board_data.ap_sys_info.mem_size = 1971200
 [11] device_detail.static_info.board_data_opt.antenna_type = BSN_INT_ANT_AP
 [12] device_detail.static_info.board_data_opt.wtp_type = BSN_AP_STANDARD
 [13] device_detail.static_info.board_data_opt.remote = true
 [14] device_detail.static_info.board_data_opt.join_priority = 1
 [15] device_detail.static_info.descriptor_data.max_radio_slots = 2
 [16] device_detail.static_info.descriptor_data.radio_slots_in_use = 2
 [17] device_detail.static_info.descriptor_data.encryption_capabilities = true
 [18] device_detail.static_info.ap_prov.is_universal = false
 [19] device_detail.static_info.ap_prov.universal_prime_status = Unprimed
 [20] device_detail.static_info.ap_models.model = C9115AXI-B
 [21] device_detail.static_info.ap_models.ap_model_short = 9115AXI
 [22] device_detail.static_info.num_ports = 1
 [23] device_detail.static_info.num_slots = 2
 [24] device_detail.static_info.wtp_type = 83
 [25] device_detail.static_info.wtp_model_type = 90
 [26] device_detail.static_info.ap_capability = [
        BRIDGE_MODE_CAPABLE,
        CAP_THREE_SPATIAL_STREAMS_CAPABLE,
        ANTENNA_SELECTION_RESTRICTED_CAPABLE,
        AVC_FNF_CAPABLE,
        RXSOP_THRESHOLD_CAPABLE,
        FABRIC_CAPABILITY,
        BARBADOS_INTERNAL_ANTENNA_SKU_CAPABLE,
        REMOTE_LAN_CAPABLE,
        DOT11AC_160MHZ_CHANNEL_WIDTH_CAPABLE,
        AVC_FNF_FABRIC_CAPABLE,
        AP_CTS_CAPABLE,
        AP_QCA_SPECTRUM_INTELLIGENCE_CAPABLE,
        FIPS_CAPABLE,
        IS_DOT1X_PORT_AUTH_CAPABLE,
        AP_TRACING_CAPABLE,
        AP_WPA3_CAPABLE,
        OFFICE_EXTEND_CAPABLE,
        ETH2_RLAN_CAPABLE,
        AP_MEWLC_CAPABLE,
        SNIFFER_MODE_CAPABLE,
        ICAP_PARTIAL_PACKET_TRACE_CAPABLE,
        ICAP_ANOMALY_DETECTION_CAPABLE,
        ICAP_STATISTICS_CAPABLE,
        ICAP_FEATURE_CAPABLE,
        AP_AWIPS_CAPABLE,
        IOX_HARDWARE_CAPABLE,
        AUX_CLIENT_INTERFACE_CAPABLE,
        CLICKOS_FEATURE_SET,
        AP_TRAFFIC_DISTRIBUTION_STATISTICS_CAPABLE
]

 [27] device_detail.static_info.remote_lan.num_rlan_ports = 0
 [28] device_detail.static_info.remote_lan.rlan_slot_id = 0
 [29] device_detail.static_info.remote_lan.rlan_port_can_be_zero = false
 [30] device_detail.static_info.is_cisco_ap = true
 [31] device_detail.static_info.is_mm_opt = false
 [32] device_detail.static_info.ap_image_name =
 [33] device_detail.dynamic_info.ap_crash_data.ap_crash_file =
 [34] device_detail.dynamic_info.ap_crash_data.ap_radio_2g_crash_file =
 [35] device_detail.dynamic_info.ap_crash_data.ap_radio_5g_crash_file =
 [36] device_detail.dynamic_info.led_brightness_level = 8
```

```
 [37] device_detail.dynamic_info.led_state_enabled = true
 [38] device_detail.dynamic_info.reset_button_state = false
 [39] device_detail.dynamic_info.led_flash_enabled = true
 [40] device_detail.dynamic_info.flash_sec = 0
 [41] device_detail.dynamic_info.temp_info.degree = 0
 [42] device_detail.dynamic_info.temp_info.temp_status = AP_TEMP_STATUS_NORMAL
 [43] device_detail.dynamic_info.temp_info.heater_status =
AP_TEMP_HEATER_STATUS_BOTH_HEATERS_OFF
 [44] device_detail.wtp_version.backup_sw_version.version = 17
 [45] device_detail.wtp_version.backup_sw_version.release = 7
 [46] device_detail.wtp_version.backup_sw_version.maint = 1
 [47] device_detail.wtp_version.backup_sw_version.build = 11
 [48] device_detail.wtp_version.backup_sw_version.stringified_ver_info = 17.7.1.11
 [49] device_detail.wtp_version.mini_ios_version.version = 0
 [50] device_detail.wtp_version.mini_ios_version.release = 0
 [51] device_detail.wtp_version.mini_ios_version.maint = 0
 [52] device_detail.wtp_version.mini_ios_version.build = 0
 [53] device_detail.wtp_version.mini_ios_version.stringified_ver_info =
 [54] device_detail.wtp_version.hw_ver.version = 1
 [55] device_detail.wtp_version.hw_ver.release = 0
 [56] device_detail.wtp_version.hw_ver.maint = 0
 [57] device_detail.wtp_version.hw_ver.build = 0
 [58] device_detail.wtp_version.hw_ver.stringified_ver_info = 1.0.0.0
 [59] device_detail.wtp_version.sw_ver.version = 17
 [60] device_detail.wtp_version.sw_ver.release = 3
 [61] device_detail.wtp_version.sw_ver.maint = 5
 [62] device_detail.wtp_version.sw_ver.build = 43
 [63] device_detail.wtp_version.sw_ver.stringified_ver_info = 17.3.5.43
 [64] device_detail.wtp_version.boot_ver.version = 1
 [65] device_detail.wtp_version.boot_ver.release = 1
 [66] device_detail.wtp_version.boot_ver.maint = 2
 [67] device_detail.wtp_version.boot_ver.build = 4
 [68] device_detail.wtp_version.boot_ver.stringified_ver_info = 1.1.2.4
 [69] device_detail.wtp_version.sw_version = 17.3.5.43
 [70] ap_lag_enabled = false
 [71] ap_location.floor = 0
 [72] ap_location.location = default location
 [73] ap_services.monitor_mode_opt_type = ENM_MODE_TYPE_NONE
 [74] ap_services.ap_dhcp_server.is_dhcp_server_enabled = false
 [75] ap_services.sniffer_ap_ifid = 0
 [76] tag_info.misconfigured_tag = APMGR_TAGS_CONFIGURED
 [77] tag_info.tag_source = EWLC_TAG_SRC_DEFAULT
 [78] tag_info.is_ap_misconfigured = false
 [79] tag_info.is_policy_tag_misconfigured = false
 [80] tag_info.is_site_tag_misconfigured = false
 [81] tag_info.is_rf_tag_misconfigured = false
 [82] tag_info.is_flex_profile_misconfigured = false
 [83] tag_info.is_ap_profile_misconfigured = false
 [84] tag_info.is_rf_profile_24_misconfigured = false
 [85] tag_info.is_rf_profile_5_misconfigured = false
 [86] tag_info.is_ap_tag_registration_done = true
 [87] tag_info.resolved_tag_info.resolved_policy_tag = default-policy-tag
 [88] tag_info.resolved_tag_info.resolved_site_tag = default-site-tag
 [89] tag_info.resolved_tag_info.resolved_rf_tag = default-rf-tag
 [90] tag_info.policy_tag_info.policy_tag_name = default-policy-tag
 [91] tag_info.site_tag.site_tag_name = default-site-tag
 [92] tag_info.site_tag.ap_profile = default-ap-profile
 [93] tag_info.site_tag.flex_profile = default-flex-profile
 [94] tag_info.rf_tag.rf_tag_name = default-rf-tag
 [95] tag_info.rf_tag.dot11a_rf_profile = default_rf_5gh
 [96] tag_info.rf_tag.dot11b_rf_profile = default_rf_24gh
 [97] tag_info.filter_info.filter_name =
 [98] tunnel.preferred_mode = PREFERRED_MODE_IPV4
 [99] tunnel.udp_lite = IPV6_CAPWAP_UDPLITE_UNCONFIG
```

```
 [100] external_module_data.xm_data.is_module_present = false
 [101] external_module_data.xm_data.enable = true
 [102] external_module_data.xm_data.xm.goodness_field = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [103] external_module_data.xm_data.xm.numeric_id = 12
 [104] external_module_data.xm_data.xm.version = [
        0,
        0
]

 [105] external_module_data.xm_data.xm.product_id = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [106] external_module_data.xm_data.xm.serial_number = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [107] external_module_data.xm_data.xm.max_power = 0
 [108] external_module_data.xm_data.xm.eeprom_size = [
```

```
        0,
        0,
        0,
        0
]

 [109] external_module_data.xm_data.xm.xm_cookie_version = 0
 [110] external_module_data.xm_data.xm.inventory.prod_id = C9115AXI-B
 [111] external_module_data.xm_data.xm.inventory.ver_id = 05
 [112] external_module_data.xm_data.xm.inventory.serial_num = FJC25331LCY
 [113] external_module_data.xm_data.xm.inventory.ent_name = C9115AX
 [114] external_module_data.xm_data.xm.inventory.ent_desc = Cisco Catalyst 9115AX Series
(IEEE 802.11ax) Access Point
 [115] external_module_data.xm_data.xm.module_name =
 [116] external_module_data.xm_data.xm.version_string =
 [117] external_module_data.xm_data.xm.serial_number_string =
 [118] external_module_data.xm_data.xm.product_id_string =
 [119] external_module_data.xm_data.xm.module_type =
 [120] external_module_data.xm_data.xm.module_description =
 [121] external_module_data.xm_data.xm.module_capabilities =
 [122] external_module_data.xm_data.xm.module_state =
 [123] external_module_data.usb_data.is_module_present = false
 [124] external_module_data.usb_data.enable = true
 [125] external_module_data.usb_data.xm.goodness_field = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [126] external_module_data.usb_data.xm.numeric_id = 12
 [127] external_module_data.usb_data.xm.version = [
        0,
        0
]

 [128] external_module_data.usb_data.xm.product_id = [
        85,
        110,
        107,
        110,
        111,
        119,
        110,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
```

```
        0,
        0,
        0
]

 [129] external_module_data.usb_data.xm.serial_number = [
        85,
        110,
        107,
        110,
        111,
        119,
        110,
        0,
        0,
        0,
        0
]

 [130] external_module_data.usb_data.xm.max_power = 0
 [131] external_module_data.usb_data.xm.eeprom_size = [
        0,
        0,
        0,
        0
]

 [132] external_module_data.usb_data.xm.xm_cookie_version = 0
 [133] external_module_data.usb_data.xm.inventory.prod_id =
 [134] external_module_data.usb_data.xm.inventory.ver_id =
 [135] external_module_data.usb_data.xm.inventory.serial_num =
 [136] external_module_data.usb_data.xm.inventory.ent_name =
 [137] external_module_data.usb_data.xm.inventory.ent_desc =
 [138] external_module_data.usb_data.xm.module_name = Unknown
 [139] external_module_data.usb_data.xm.version_string = V00
 [140] external_module_data.usb_data.xm.serial_number_string = Unknown
 [141] external_module_data.usb_data.xm.product_id_string = Unknown
 [142] external_module_data.usb_data.xm.module_type = USB Module
 [143] external_module_data.usb_data.xm.module_description = Unknown
 [144] external_module_data.usb_data.xm.module_capabilities =
 [145] external_module_data.usb_data.xm.module_state = Not Detected
 [146] external_module_data.usb_override = false
 [147] external_module_data.is_ext_module_enabled = false
 [148] external_module_data.expansion_module_extended_info.power_sufficient = 0
 [149] external_module_data.expansion_module_extended_info.antenna_product_id = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
```

```
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [150] external_module_data.expansion_module_extended_info.antenna_serial_number = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [151] external_module_data.expansion_module_extended_info.antenna_prod_ID =
 [152] ipv6_joined = 0
 [153] wtp_ip_addr = 10.22.243.229
 [154] ap_state.ap_admin_state = ENM_ADMINSTATE_ENABLED
 [155] ap_state.ap_operation_state = EWLC_ENM_AP_STATE_REG
 [156] ap_mode_data.home_ap_enabled = false
 [157] ap_mode_data.clear_mode = false
 [158] ap_mode_data.ap_sub_mode = AP_SUB_MODE_NONE
 [159] ap_mode_data.wtp_mode = EWLC_ENM_SPAM_AP_MODE_LOCAL
 [160] ap_mode_data.ap_fabric_data.is_fabric_ap = false
 [161] ap_mode_data.ap_fabric_data.lisp_state = EWLC_ENM_LISP_QUERY_NOT_NEEDED
 [162] ap_time_info.boot_time = Fri, 05 Aug 2022 06:47:33 +0000
```

```
 [163] ap_time_info.join_time = Fri, 05 Aug 2022 06:50:13 +0000
 [164] ap_time_info.join_time_taken = 159
 [165] ap_time_info.last_up_time = 1
 [166] country_code = US
 [167] ap_security_data.lsc_provision_inprogress = false
 [168] ap_security_data.fips_enabled = false
 [169] ap_security_data.wlancc_enabled = false
 [170] ap_security_data.cert_type = EWLC_CERT_MIC
 [171] ap_security_data.lsc_ap_auth_type = EWLC_ENM_LSC_AP_AUTH_CAPWAP_DTLS
 [172] num_radio_slots = 2
 [173] dart_is_connected = false
 [174] dart_is_connected_str = Not Connected
 [175] is_master = false
 [176] sliding_window.multi_window_support = true
 [177] sliding_window.window_size = 1
 [178] ap_vlan.vlan_tag_state = VLAN_TAGGING_DISABLED
 [179] ap_vlan.vlan_tag_id = 0
 [180] capwap_iifid = 2415919114
 [181] hyperlocation_data.hyperlocation_method = HYPERLOCATION_METHOD_NONE
 [182] hyperlocation_data.per_ap_hl_tlv_rcvd = HYPERLOCATION_AP_TLV_RECEIVED
 [183] hyperlocation_data.cmx_ip = null
 [184] cdp_enable = true
 [185] cdp_cache_index_list.buffer = [
        1,
        0,
        0,
        0
]

 [186] ap_stationing_type = EWLC_ENM_INDOOR_AP
 [187] int_if_num = 0
 [188] radio_key = [
        {wtp_mac : 1CD1.E065.C340, radio_slot_id : 0},
        {wtp_mac : 1CD1.E065.C340, radio_slot_id : 1},
        {wtp_mac : 0000.0000.0000, radio_slot_id : 0},
        {wtp_mac : 0000.0000.0000, radio_slot_id : 0}
]

 [189] reboot_stats.reboots = 9
 [190] reboot_stats.ac_initiated = 4
 [191] reboot_stats.link_failure = 0
 [192] reboot_stats.sw_failure = 0
 [193] reboot_stats.hw_failure = 0
 [194] reboot_stats.unknown_failure = 0
 [195] reboot_stats.reboot_reason = AP_REBOOT_REASON_IMG_UPGRADE
 [196] reboot_stats.reboot_types = AP_REBOOT_SPAM_INITIATED
 [197] reboot_stats.reboot_type = AP_REBOOT_SPAM_INITIATED
 [198] slot_type = [
        0,
        0,
        0,
        0
]

 [199] mesh_profile_inuse =
 [200] mesh_ap_role = ENM_EWLC_AP_ROLE_MESH
 [201] wtp_cfg_reval_data.wtp_revalidate = false
 [202] wtp_cfg_reval_data.pending_wtp_notifies = 0
 [203] me_internal_ap = false
 [204] ap_type = AP_TYPE_CAPWAP
 [205] is_mewlc_candidate = false
 [206] is_invalid_master = false
 [207] is_callback_success = false
 [208] proxy_info.hostname =
```

```
 [209] proxy_info.port = 0
 [210] proxy_info.no_proxy_list =
 [211] grpc_enabled = true
 [212] ap_image_size = 0
 [213] ap_cur_bytes = 0
 [214] image_size_eta = 0
 [215] image_size_start_time = Thu, 01 Jan 1970 00:00:00 +0000
 [216] image_size_percentage = 0
 [217] dual_dfs_capable = false
 [218] mdns_group_id = 0
 [219] mdns_rule_name =
 [220] ap_keepalive_state = true
 [221] local_dhcp = false
 [222] ipv4_pool.network = 0.0.0.0
 [223] ipv4_pool.lease_time = 0
 [224] ipv4_pool.netmask = 0.0.0.0
 [225] wlc_image_size_eta = 0
 [226] wlc_image_size_start_time = Thu, 01 Jan 1970 00:00:00 +0000
 [227] wlc_image_size_percentage = 0
 [228] matching_ewc_image = false
 [229] disconnect_detail.ext_disconnect_reason_capable = false
 [230] disconnect_detail.disconnect_reason = UNKOWN
 [231] antenna_monitor.support = false
 [232] antenna_monitor.enabled = false
 [233] antenna_monitor.rssi_fail_threshold = 0
 [234] antenna_monitor.weak_rssi = 0
 [235] antenna_monitor.detection_time = 0
 [236] wtp_ip = 10.22.243.229
}
```

How do I view the current TDL values for an AP?

1. Execute the command on the wireless controller to retrieve the current configuration for an AP:

   `test platform software database get ewlc_oper/ble_ltx_ap;ap_mac=<mac-without-dots>`

   Replace <*mac-without-dots*> with the actual MAC address of the AP, removing any periods. For example:

   ```
   wireless controller# test platform software database get
   ewlc_oper/ble_ltx_ap;ap_mac=04eb409ec3c0
   ```

The output presents a list of parameters, such as:

- The AP's MAC address, without any delimiters.
- The administrative state of the AP.
- Details of the scan configuration, including intervals and states.
- Settings for the iBeacon and Eddystone profiles.
- Information on viBeacons profiles.
- Statistics on the types of scans performed.
- Host device data, such as the name and BLE MAC address.
- Current feature modes and the operational status of the device.
- Capabilities of the device, including support for technologies like BLE and Zigbee.

Each parameter provides details including the last report time and the validity of the status.

```
wireless controller# test platform software database get
ewlc_oper/ble_ltx_ap;ap_mac=04eb409ec3c0
Table Record Index 0 = {
 [0] ap_mac = 04EB.409E.C3C0
 [1] admin.state = BLE_LTX_ADMIN_STATE_ON
 [2] admin.feedback.state_status = 0
 [3] admin.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [4] admin.report.valid = true
 [5] scan_config.interval_sec = 1
 [6] scan_config.state = BLE_LTX_SCAN_STATE_ON
 [7] scan_config.max_value = 8
 [8] scan_config.window_msec = 800
 [9] scan_config.filter = BLE_LTX_SCAN_FILTER_ON
 [10] scan_config.feedback.interval_sec_status = 0
 [11] scan_config.feedback.state_status = 0
 [12] scan_config.feedback.max_value_status = 0
 [13] scan_config.feedback.window_msec_status = 0
 [14] scan_config.feedback.filter_status = 0
 [15] scan_config.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [16] scan_config.report.valid = true
 [17] profile_ibeacon.uuid = 00000000-0000-0000-0000-000000000000
 [18] profile_ibeacon.major = 0
 [19] profile_ibeacon.minor = 0
 [20] profile_ibeacon.tx_power = 0
 [21] profile_ibeacon.frequency_msec = 0
 [22] profile_ibeacon.adv_tx_power = 65
 [23] profile_ibeacon.feedback.uuid_status = 0
 [24] profile_ibeacon.feedback.major_status = 0
 [25] profile_ibeacon.feedback.minor_status = 0
 [26] profile_ibeacon.feedback.tx_power_status = 0
 [27] profile_ibeacon.feedback.frequency_msec_status = 0
 [28] profile_ibeacon.feedback.adv_tx_power_status = 0
 [29] profile_ibeacon.report.last_report_time = Fri, 05 Jun 2020 02:18:30 +0000
 [30] profile_ibeacon.report.valid = true
 [31] profile_eddy_url.url =
 [32] profile_eddy_url.feedback.url_status = 0
 [33] profile_eddy_url.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [34] profile_eddy_url.report.valid = false
 [35] profile_eddy_uid.namespace =
 [36] profile_eddy_uid.instance_id =
 [37] profile_eddy_uid.feedback.namespace_status = 0
 [38] profile_eddy_uid.feedback.instance_id_status = 0
 [39] profile_eddy_uid.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [40] profile_eddy_uid.report.valid = false
 [41] profile_vibeacons.common.interval_msec = 0
 [42] profile_vibeacons.common.feedback.interval_msec_status = 0
 [43] profile_vibeacons.common.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [44] profile_vibeacons.common.report.valid = false
 [45] profile_vibeacons.vibeacons = [
        {beacon_id : 0, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false},
        {beacon_id : 1, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
```

```
report.valid : false},
        {beacon_id : 2, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false},
        {beacon_id : 3, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false},
        {beacon_id : 4, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false}
]

 [46] profile_vibeacons.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [47] profile_vibeacons.report.valid = false
 [48] scan_counters.total = 0
 [49] scan_counters.dna_ltx = 0
 [50] scan_counters.system_tlm = 0
 [51] scan_counters.event_tlm = 0
 [52] scan_counters.regular_tlm = 0
 [53] scan_counters.emergency = 0
 [54] scan_counters.event_emergency = 0
 [55] scan_counters.other = 0
 [56] scan_counters.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [57] scan_counters.report.valid = true
 [58] host_data.device_name = Developme
 [59] host_data.ble_mac = 806F.B031.E024
 [60] host_data.api_version = 1
 [61] host_data.fw_version = FF020710
 [62] host_data.advertise_count = 0
 [63] host_data.uptime_dsec = 10
 [64] host_data.active_profile = BLE_LTX_PROFILE_NO_ADV
 [65] host_data.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [66] host_data.report.valid = true
 [67] feature_mode.feature = BLE_LTX_FEATURE_ZIGBEE
 [68] feature_mode.mode = BLE_LTX_MODE_IOX
 [69] feature_mode.report.last_report_time = Fri, 05 Jun 2020 07:26:19 +0000
 [70] feature_mode.report.valid = true
 [71] device_status.device = BLE_LTX_DEVICE_MSM1
 [72] device_status.state = BLE_LTX_DEVICE_STATE_IOX_BLE_MODE
 [73] device_status.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [74] device_status.report.valid = true
 [75] capability.ble = true
 [76] capability.zigbee = true
 [77] capability.thread = false
 [78] capability.usb = true
 [79] capability.report.last_report_time = Wed, 03 Jun 2020 08:08:20 +0000
 [80] capability.report.valid = true
}
```

How do I get the telemetry connection status?

This procedure shows you how to check the telemetry connection status.

1. Enter the command:

   ```
   show telemetry internal protocol cloud-native manager <connector-ip-address> 8004
   source-address <source-IP-address>
   ```

   Replace <*connector-ip-address*> with the IP address of the connector and <*source-IP-address*> with the source IP address of your wireless controller.

2. In the output displayed, look for the **State** field to determine the telemetry connection status.

The following is a sample output of the command. The **State** is **CNDP_STATE_CONNECTED** and that indicates that the connection is successfully established

```
wireless controller# show telemetry internal protocol cloud-native manager 10.22.243.53
8004 source-address 10.22.243.52
Telemetry protocol manager stats:

Con str                : 10.22.243.53:8004:0:10.22.243.52
Sockfd                 : 97
Protocol               : cloud-native
State                  : CNDP_STATE_CONNECTED
Table id               : 0
Wait Mask              :
Connection Retries     : 0
Send Retries           : 0
Pending events         : 0
Session requests       : 1
Session replies        : 1
Source ip              : 10.22.243.52
Bytes Sent             : 1121093
Msgs Sent              : 17613
Msgs Received          : 0
Creation time:         : Wed Jun  3 23:16:22:830
Last connected time:   : Wed Jun  3 23:16:22:892
Last disconnect time:  :
Last error:            :
Connection flaps:      : 0
Last flap Reason:      :
Keep Alive Timeouts:   : 0
Last Transport Error   : No Error
```

How do I view IOx AP state and mode?

To view the Bluetooth Low Energy (BLE) state and mode for each AP connected to the wireless controller, you can perform the following steps:

1. On the wireless controller, enter the following command:

   ```
   show ap ble summary
   ```

The following example shows how to view the BLE state and mode for each AP.

This output provides a summary of each AP's BLE status, indicating whether it is active (**Up**) and the current BLE mode, which is **IOx** for all APs in this example.

```
wireless-controller# show ap ble summary
AP Name                          BLE AP State          BLE mode
-----------------------------------------------------------------
AP_10.2830                       Up                    IOx
AP_02.2898                       Up                    IOx
AP_06.28CC                       Up                    IOx
AP_08.28E0                       Up                    IOx
AP_07.28E4                       Up                    IOx
AP_09.28EC                       Up                    IOx
AP_01.28F0                       Up                    IOx
AP_03.2928                       Up                    IOx
AP_05.2934                       Up                    IOx
AP_04.2938                       Up                    IOx
```

How do I view gRPC details?

To view detailed gRPC (gRPC Remote Procedure Calls) statistics for a specific Access Point (AP), follow these steps:

1. Run the following command after replacing the <*AP Name*>:

   ```
   show ap name <AP Name> grpc detail
   ```

2. The output provides detailed gRPC statistics for the specified AP.

   In this output, the **gRPC channel status** indicates whether the connection is active (**Up**). The output also shows various packet statistics such as transmit attempts, transmit failures, packets received, and receive failures.

   The following is a sample output of the command:

   ```
   wireless-controller# show ap name ap-name grpc detail

   gRPC channel status        : Up
   Packets transmit attempts  : 818411
   Packets transmit failures  : 2651788
   Packets receive count      : 2711
   Packets receive failures   : 0
   ```

How do I view AP BLE configuration details?

To understand the Bluetooth Low Energy (BLE) configuration details for an AP, you can examine the output provided by your wireless controller. Run the following command, and replace <*ap-name*>.

```
show ap name <ap-name> ble detail
```

The command displays the detailed BLE configuration settings for an AP.

```
wireless-controller# show ap name ap-name grpc detail

Mode report time          : 06/25/2020 21:30:54
Mode                      : Advanced (IOx)
Radio mode                : BLE
Admin state report time   : 06/25/2020 21:31:14
Admin state               : Up
Interface report time     : 06/25/2020 21:30:58
Interface                 : MSM1
Interface state           : Open
Type                      : Integrated
```

```
Capability report time    : 06/25/2020 21:16:25
Capability                : BLE, Zigbee, USB,
Host data report time     : 06/25/2020 21:31:14
Host data
  Device name                 : AP_102830
  Dot15 Radio MAC             : 18:04:ed:c5:02:bc
  API version                 : 256
  FW version                  : 2.7.16
  Broadcast count             : -1844445184
  Uptime                      : 838860800 deciseconds
  Active profile              : No Advertisement
Scan Statistics report time    : 06/25/2020 21:30:36
Scan statistics
  Total scan records          : 0
Scan role report time  : 06/25/2020 21:31:14
Scan role
  Scan state                  : Enable
  Scan interval               : 1 seconds
  Scan window                 : 800 milliseconds
  Scan max value              : 8
  Scan filter                 : Enable
Broadcaster role
  Current profile type: iBeacon
  Last report time            : N/A
    UUID                      : Unknown
    Major                     : Unknown
    Minor                     : Unknown
    Transmit power            : Unknown
    Frequency                 : Unknown
    Advertised transmit power : Unknown
  Current profile type: Eddystone URL
  Last report time            : 06/25/2020 21:27:50
    URL                       : http://dnaspaces.io/edm
  Current profile type: Eddystone UID
  Last report time            : N/A
    Namespace                 : Unknown
    Instance id               : Unknown
  Current profile type: viBeacon
  Last report time            : N/A
    Interval                  : Unknown
    Beacon ID                 : 0
      UUID                      : Unknown
      Major                     : Unknown
      Minor                     : Unknown
      Transmit power            : Unknown
      Advertised transmit power : Unknown
      Enable                    : Unknown
    Beacon ID                 : 1
      UUID                      : Unknown
      Major                     : Unknown
      Minor                     : Unknown
      Transmit power            : Unknown
      Advertised transmit power : Unknown
      Enable                    : Unknown
    Beacon ID                 : 2
      UUID                      : Unknown
      Major                     : Unknown
      Minor                     : Unknown
      Transmit power            : Unknown
      Advertised transmit power : Unknown
      Enable                    : Unknown
    Beacon ID                 : 3
      UUID                      : Unknown
      Major                     : Unknown
```

```
    Minor                     : Unknown
    Transmit power            : Unknown
    Advertised transmit power : Unknown
    Enable                    : Unknown
  Beacon ID                 : 4
    UUID                      : Unknown
    Major                     : Unknown
    Minor                     : Unknown
    Transmit power            : Unknown
    Advertised transmit power : Unknown
    Enable                    : Unknown
```

Some of the output descriptors are described below:

1. **Mode Report Time:** This timestamp, **06/25/2020 21:30:54**, indicates when the AP mode was last reported.
2. **Mode:** The AP is set to an **Advanced (IOx)** operational mode.
3. **Radio Mode:** The radio is operating in **BLE** mode.
4. **Admin State Report Time:** As of **06/25/2020 21:31:14**, the administrative state of the AP was last reported.
5. **Admin State:** The AP is currently **Up** and operational.
6. **Interface Report Time:** The interface status was last reported on **06/25/2020 21:30:58**.
7. **Interface:** The interface identifier is **MSM1**.
8. **Interface State:** The interface is **Open** for connections.
9. **Type:** The AP has an **Integrated** interface type.
10. **Capability Report Time:** The capabilities were last reported on **06/25/2020 21:16:25**.
11. **Capability:** The AP supports **BLE**, **Zigbee**, and **USB** functionalities.
12. **Host Data Report Time:** This timestamp, **06/25/2020 21:31:14**, shows when the host data was last reported.
13. **Host Data:** It includes the AP's name **AP_102830**, its Dot15 radio MAC address **18:04:ed:c5:02:bc**, API version **256**, firmware version **2.7.16**, and other operational details.
14. **Scan Statistics Report Time:** The scan statistics were last reported on **06/25/2020 21:30:36**.
15. **Scan Statistics:** Indicates no total scan records are available.
16. **Scan Role Report Time:** The scan role was last reported on **06/25/2020 21:31:14**.
17. **Scan Role:** The AP is set to enable scanning with a **1-second** interval and an **800-millisecond** window. The maximum value is **8** and the scan filter is enabled.

How do I view the current TDL values for AP air quality?

To view the current Total Dissolved Load (TDL) values for AP air quality, perform the following steps:

1. Run the command to retrieve the TDL values:

```
test platform software database get-n all ewlc_oper/ap_air_quality
```

2. The command displays the current TDL values for all APs with air quality sensors. For example:

```
wireless controller# test platform software database get-n all ewlc_oper/ap_air_quality
Table Record Index 0 = {
[0] ap_mac = 687D.B45E.E7C0
[1] last_update = Tue, 12 Oct 2021 15:08:19 +0530
[2] rmox_0 = 5.62121e+07
[3] rmox_1 = 6.12815e+06
[4] rmox_2 = 1.26038e+06
[5] rmox_3 = 579564
[6] rmox_4 = 398259
[7] rmox_5 = 280246
[8] rmox_6 = 201467
[9] rmox_7 = 370324
[10] rmox_8 = 680235
[11] rmox_9 = 1.29709e+06
[12] rmox_10 = 3.18129e+06
[13] rmox_11 = 1.06436e+07
[14] rmox_12 = 6.10561e+07
[15] iaq = 1
[16] etoh = 0.0094
[17] eco2 = 400.212
[18] tvoc = 0.0178
}
```

In this example, the output provides the air quality data for an AP, including the MAC address, last update time, various rmox values, indoor air quality (iaq), ethanol (etoh), equivalent carbon dioxide (eco2), and total volatile organic compounds (tvoc).

How do I view the current TDL values for AP temperature and humidity?

To view the current Total Dissolved Load (TDL) values for AP temperature and humidity, please follow these steps:

1. Execute the command to fetch the TDL values for temperature and humidity:

```
test platform software database get-n all ewlc_oper/ap_temp
```

2. This command shows the TDL values for all APs equipped with temperature and humidity sensors. For example:

```
wireless controller# test platform software database get-n all ewlc_oper/ap_temp

Table Record Index 0 = {
[0] ap_mac = 687D.B45E.E7C0
[1] last_update = Tue, 12 Oct 2021 15:08:19 +0530
[2] temp = 233.382
[3] humidity = 0
}
```

In this example, the output lists the temperature and humidity values, along with the MAC address of the AP and the last update timestamp.