排除接入點與控制器的關聯故障

目錄

簡介

本檔案介紹使用案例，以瞭解存取點(AP)和無線LAN控制器(WLC)之間控制和布建無線存取點(CAPWAP)/輕量存取點通訊協定(LWAPP)通道中斷的原因。

必要條件

需求

思科建議您瞭解AP和控制器配置，以及路由和交換的基本知識。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

基於控制器的AP註冊流程

AP通過上述過程向控制器註冊：

1. 從AP向WLC發出的CAPWAP發現消息請求。
2. 從WLC到AP的發現響應消息。
3. AP根據收到的CAPWAP響應選擇WLC加入。
4. 從AP傳送到WLC的加入請求。
5. 控制器驗證AP並傳送加入響應。

向WLC註冊時在AP上捕獲的日誌：

```
Press RETURN to get started!

Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

    %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY

      status of voice_diag_test from WLC is false

     %SSH-5-ENABLED: SSH 2.0 has been enabled

      Logging LWAPP message to 255.255.255.255.

       %CDP_PD-4-POWER_OK: 15.4 W power - NEGOTIATED inline power source

       %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up

        %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

         %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to up
```

```
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - CLI initiated

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up Translating "CISCO-LWAPP-CONTROLLER"...don

%CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip:

peer_port: 5246

%CAPWAP-5-CHANGED: CAPWAP changed state to

%CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip:

peer_port: 5246

%CAPWAP-5-SENDJOIN: sending Join Request to

%CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
```

```
%CAPWAP-5-CHANGED: CAPWAP changed state to CFG

%LWAPP-3-CLIENTERRORLOG: Operator changed mode for 802.11g. Rebooting.

%LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down

%SYS-5-RELOAD: Reload requested by CAPWAP CLIENT. Reload Reason: Operator changed mode for 802.11g.

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down IOS Bootloader - Starting system.
```

使用案例1

1. AP與WLC取消關聯，並且從交換機驗證後，顯示AP沒有IP。

通過控制檯連線到AP時記錄：

```
LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
```

```
%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!
```

解決方案：

如果DHCP伺服器位於遠端位置，請修復在VLAN下配置的IP幫助地址的可達性問題。如果本地配置了DHCP，請確保沒有DHCP衝突。在AP上配置靜態IP:

登入到AP並鍵入以下命令：

```
capwap ap ip address <ip> <mask>

capwap ap ip default-gateway <ip>
```

此外，您還可以指定控制器IP位址：

```
capwap ap controller ip address
```

2.請注意，存在具有IP地址的AP，但無法與WLC通訊可能是控制器IP的解析故障。

來自AP的日誌，出現域名系統(DNS)解析失敗的問題：

```
<Date & time>  %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER.local doamin

Not in Bound state.
```

解決方案：

檢查內部DNS伺服器可訪問性（如果可接受），確保通過DHCP推送的控制器IP地址可訪問。

Break-fix：在AP上手動配置控制器。

```
"capwap ap {primary-base | secondary-base | tertiary-base}controller-name controller-ip-address"
```

3.您看到AP已在控制器上註冊，但您仍然看不到所需的服務集識別符號(SSID)廣播。

```
(4402-d) >config wlan apgroup interface-mapping add <ap group name> <wlandi> <interfacename>
```

解決方案：
請在AP組下新增無線LAN(WLAN)。

使用案例2

請注意，在交換機的思科發現協定(CDP)鄰居上未看到AP，並且AP連線的交換機處於錯誤禁用狀態。

從Switch：捕獲

```
Dec  9 08:42:35.836 UTC: RSTP(10): sending BPDU out Te3/0/47STP: pak->vlan_id: 10

Dec  9 08:42:35.836 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable stateSTP: pak->vlan_id: 1

Dec  9 09:47:32.651 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD

Dec  9 09:47:33.651 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted

Dec  9 09:47:53.545 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state

Dec  9 09:48:10.955 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD

Dec  9 09:48:11.955 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted

Dec  9 09:48:32.114 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state
```

解決方案：
在任何情況下，AP都不會傳送網橋協定資料單元(BPDU)防護，這是交換機端的問題。將AP移動到另一個空閒埠，並複製介面配置以及必要的物理檢查。

使用案例3

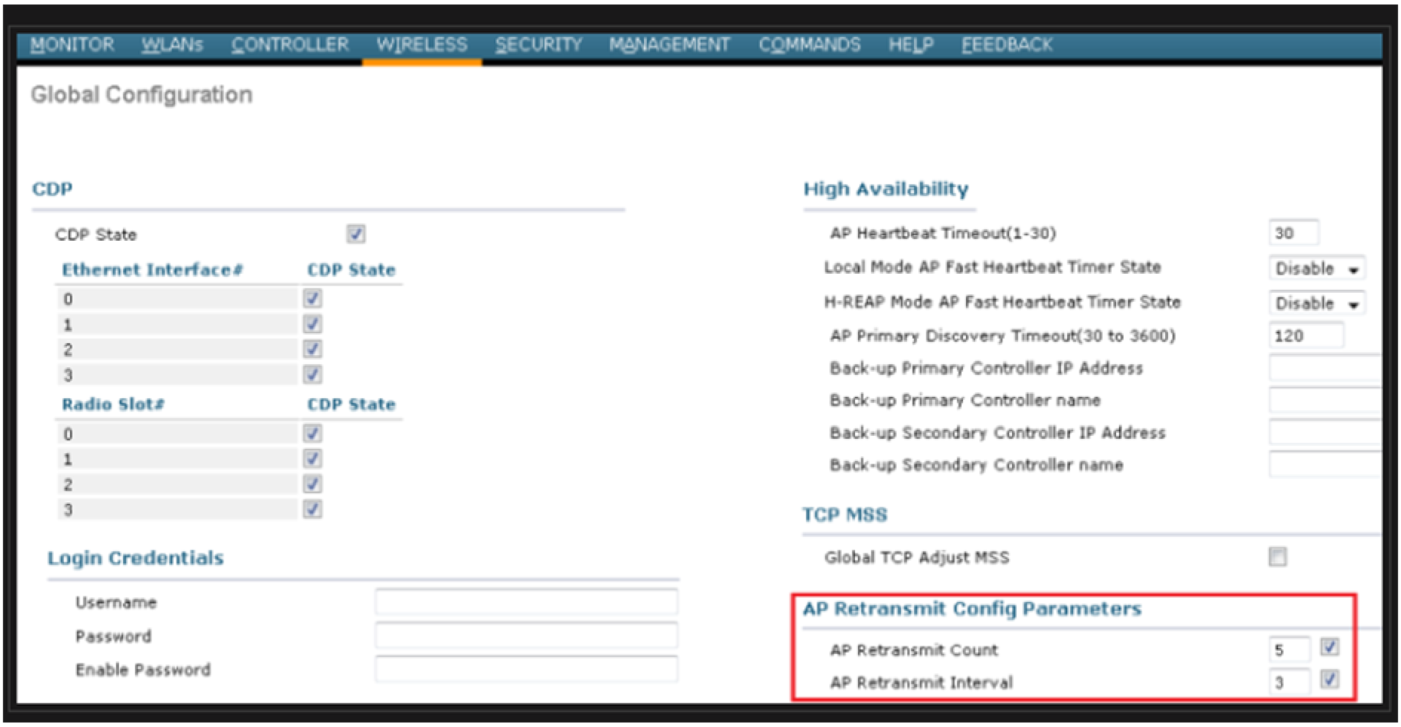
在遠端辦公室設定中，經常會看到AP和控制器之間的CAPWAP隧道隨機中斷，需要檢查的最重要引數是重新傳輸和重試間隔。

AP重新傳輸間隔和重試間隔可以在全域性級別和AP級別配置。全域性配置將這些配置引數應用到所有AP。也就是說，所有AP的重傳間隔和重試計數是一致的。

來自WLC的問題日誌：

```
*spamApTask6: Jun 01 17:17:55.426: %LWAPP-3-AP_DEL: spam_lrad.c:6088 1c:d1:e0:43:1d:20: Entry deleted for AP: 10.209.36.5 (5256) reason : AP
```

解決方案：如果問題在所有站點出現，則增加 **Retransmit count** 和 **Retransmit interval** 在wireless Global configuration下。當所有AP出現問題時增加值的選項。



Global Configuration

CDP

CDP State ☑

Ethernet Interface#	CDP State
0	☑
1	☑
2	☑
3	☑

Radio Slot#	CDP State
0	☑
1	☑
2	☑
3	☑

Login Credentials

Username
Password
Enable Password

High Availability

AP Heartbeat Timeout(1-30) 30
Local Mode AP Fast Heartbeat Timer State Disable
H-REAP Mode AP Fast Heartbeat Timer State Disable
AP Primary Discovery Timeout(30 to 3600) 120
Back-up Primary Controller IP Address
Back-up Primary Controller name
Back-up Secondary Controller IP Address
Back-up Secondary Controller name

TCP MSS

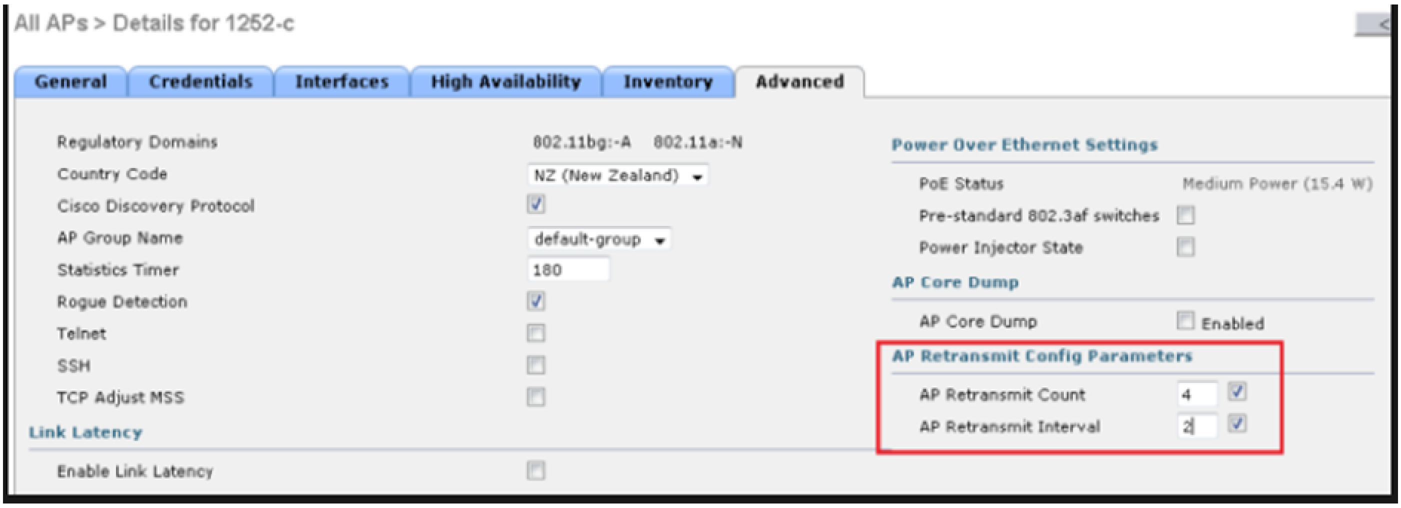
Global TCP Adjust MSS □

AP Retransmit Config Parameters

AP Retransmit Count 5 ☑
AP Retransmit Interval 3 ☑

用於在「全域性配置」下更改AP重新傳輸配置引數的選項

如果問題僅針對一個遠端站點，則增加 **Retransmit count** 和 **Retransmit interval** 在特定的AP上解決了問題。



All APs > Details for 1252-c

Regulatory Domains 802.11bg:-A 802.11a:-N
Country Code NZ (New Zealand)
Cisco Discovery Protocol ☑
AP Group Name default-group
Statistics Timer 180
Rogue Detection ☑
Telnet ☐
SSH ☐
TCP Adjust MSS ☐

Link Latency
Enable Link Latency ☐

Power Over Ethernet Settings
PoE Status Medium Power (15.4 W)
Pre-standard 802.3af switches ☐
Power Injector State ☐

AP Core Dump
AP Core Dump ☐ Enabled

AP Retransmit Config Parameters
AP Retransmit Count 4 ☑
AP Retransmit Interval 2 ☑

用於更改特定AP下的AP重新傳輸配置引數的選項

使用案例4

AP與WLC完全解除關聯，且無法重新加入控制器，這可能會與數位憑證相關。

有關Cisco WLC和AP方面的裝置證書的一些簡略說明：

- 預設情況下，思科提供的每個裝置都附帶一個有效期為10年的證書。
- 此憑證用於在Cisco WLC和AP之間執行驗證。
- 在證書的幫助下，AP和WLC建立一個安全的資料包傳輸層安全(DTLS)隧道。

遇到兩種與證書相關的問題：

問題1：舊版AP（不想加入WLC）。

通過控制檯連線到AP有助於確定問題，日誌如下所示：

```
*Sep 13 18:26:24.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.1.1 peer_port: 5246
*Sep 13 18:26:24.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Sep 13 18:26:24.099: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed.
The certificate (SN: XXXXXXXXXXXXXX) has expired.    Validity period ended on 19:56:24 UTC Aug 12 2018
*Sep 13 18:26:24.099: %LWAPP-3-CLIENTERRORLOG: Peer certificate verification failed
*Sep 13 18:26:24.099: %CAPWAP-3-ERRORLOG: Certificate verification failed!
```

問題2：較新的AP不想加入較舊的WLC。
AP的控制檯顯示的錯誤可能如下所示：

```
[*09/09/2019 04:55:26.3299] CAPWAP State: DTLS Teardown
[*09/09/2019 04:55:30.9385] CAPWAP State: Discovery
[*09/09/2019 04:55:30.9385] Did not get log server settings from DHCP.
[*09/09/2019 04:55:41.0000] CAPWAP State: DTLS Setup
[*09/09/2019 04:55:41.3399] Bad certificate alert received from peer.
[*09/09/2019 04:55:41.3399] DTLS: Received packet caused DTLS to close connection
```

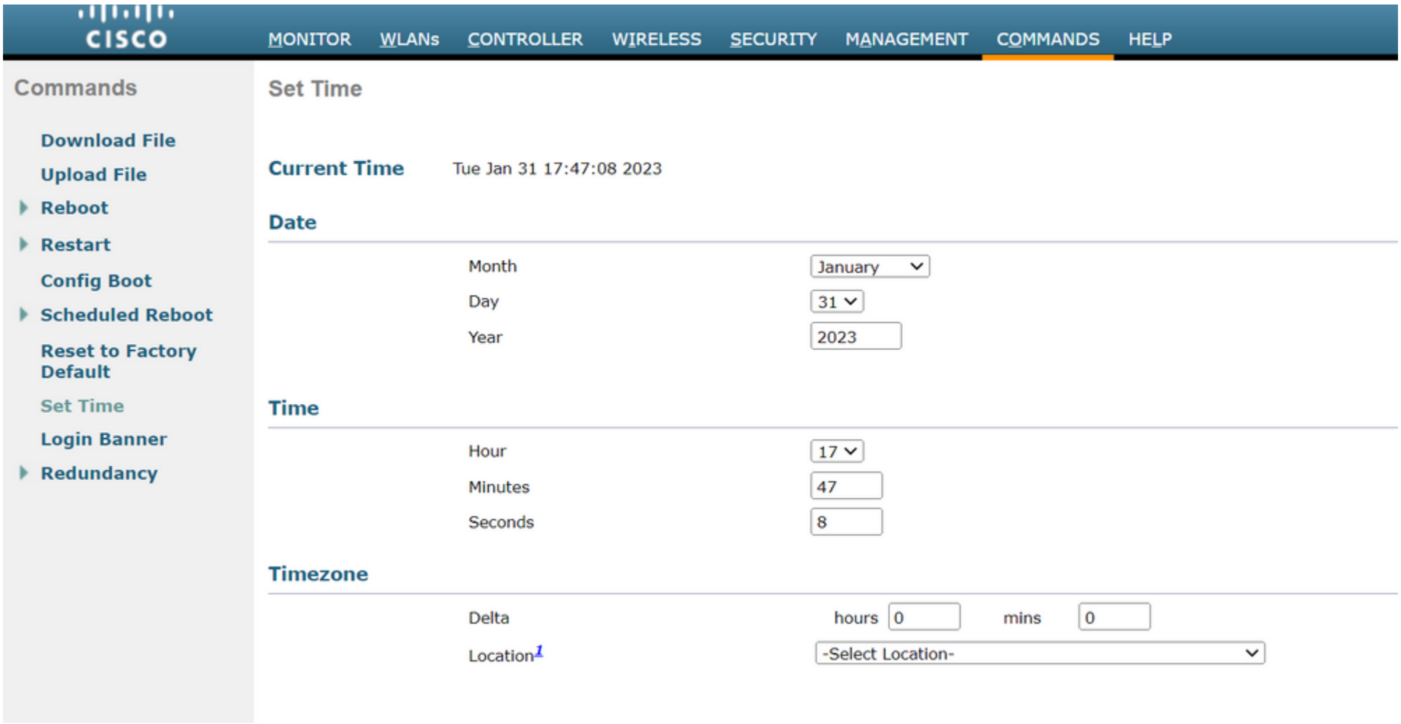
解決方案：

1. NTP通過CLI禁用和手動設定時間：

```
(Cisco Controller)> config time ntp delete 1
(Cisco Controller)> config time manual 09/30/18 11:30:00
```

2. NTP通過GUI禁用和手動設定時間：

導航至 **Controller > NTP > Server > Commands > Set Time** 以便刪除列出的NTP伺服器。



Set Time

Current Time Tue Jan 31 17:47:08 2023

Date

Month January

Day 31

Year 2023

Time

Hour 17

Minutes 47

Seconds 8

Timezone

Delta hours 0 mins 0

Location[1] -Select Location-

在GUI上手動設定時間的位置

2.停用控制器上的製造商安裝憑證(MIC)。此命令僅在最新版本上被接受。

```
(Cisco Controller)> config ap cert-expiry-ignore mic enable
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。