コントローラからのアクセスポイントの関連付け解除のトラブルシューティング

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

コントローラベースのAP登録プロセス

使用例 1

使用例 2

使用例 3

使用例 4

関連情報

はじめに

このドキュメントでは、アクセスポイント(Ap)とワイヤレスLANコントローラ(WLC)の間のCAPWAP/LWAPPトンネルの切断を理解するための使用例について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- アクセスポイント(AP)とワイヤレスLANコントローラ(WLC)の設定
- ルーティングとスイッチング.
- Control and Provisioning of Wireless Access Points(CAPWAP)
- Lightweight アクセス ポイント プロトコル (LWAPP)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、アクセスポイント(AP)とワイヤレスLANコントローラ(WLC)の間でのControl and Provisioning of Wireless Access Points(CAPWAP)/Lightweight Access Point Protocol(LWAPP)トンネルの中断の理由を理解するための使用例について説明します。

コントローラベースのAP登録プロセス

APは、コントローラに登録するために前述のプロセスを実行します。

1. APからWLCへのCAPWAPディスカバリメッセージ要求。
2. WLCからAPへのディスカバリ応答メッセージ
3. APは、受信したCAPWAP応答に基づいて、加入するWLCを選択します。
4. 接続要求がAPからWLCに送信されます。
5. コントローラはAPを検証し、加入応答を送信します。

WLCへの登録時にAPでキャプチャされたログ：

```
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"...domain server (255.255.255.255)

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

%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.

使用例 1

1. APはWLCから関連付けが解除され、スイッチから確認されると、APにIPがないことが示されます。

APにコンソール接続した場合のログ：

```
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 !!
```

ソリューション：

DHCPサーバがリモートにある場合は、VLANで設定されているIPヘルパーアドレスへの到達可能性の問題を解決してください。DHCPがローカルに設定されている場合は、DHCPの競合がないことを確認します。APでスタティックIPを設定します。

APにログインし、次のコマンドを入力します。

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

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

また、コントローラのIPアドレスも指定できます。

```
capwap ap controller ip address
```

2. IPアドレスを持つAPはありますが、WLCとの通信に失敗すると、コントローラIPの解決に失敗する可能性があることに注意してください。

ドメインネームシステム(DNS)の解決に失敗した問題を含むAPからのログ：

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

Not in Bound state.
```

ソリューション：

内部DNSサーバの到達可能性を確認します。許容可能な場合は、DHCP経由でプッシュされたコントローラIPアドレスが到達可能であることを確認します。

修正方法：APでコントローラを手動で設定します。

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

3. APがコントローラに登録されているのに、必要なService Set Identifier(SSID)のブロードキャストが表示されていないことがわかります。

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

ソリューション：
APグループの下にワイヤレスLAN(WLAN)を追加してください。

使用例 2

APがスイッチのCisco Discovery Protocol(CDP)ネイバーに表示されず、APに接続されたスイッチがerror-disabled状態になっていることに注意してください。

スイッチからキャプチャされたログ：

```
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
```

ソリューション：
どのような状況でも、APはブリッジプロトコルデータユニット(BPDU)ガードを送信しません。これはスイッチ側からの問題です。APを別の空きポートに移動し、必要な物理チェックとともにインターフェイス設定を複製します。

使用例 3

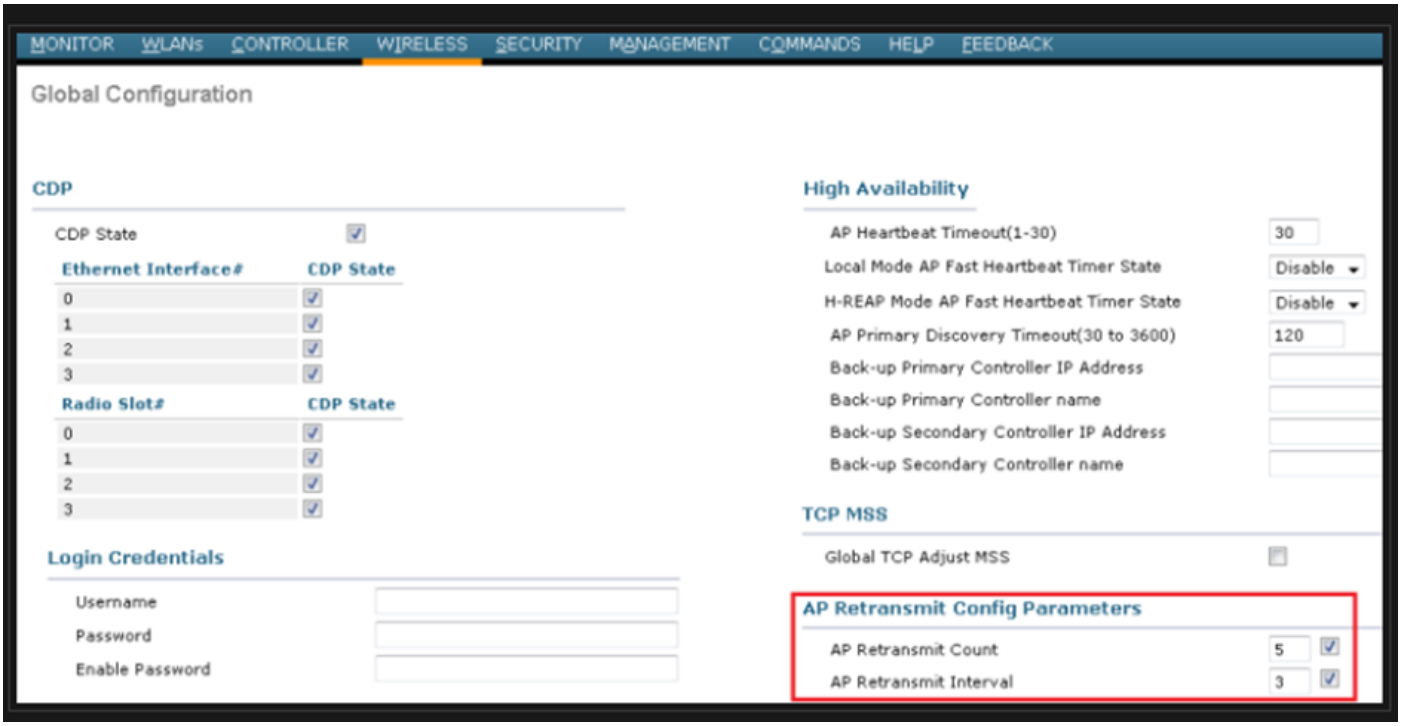
リモートオフィスのセットアップでは、APとコントローラの間でCAPWAPトンネルがランダムに切断されることが多く、最も重要な確認パラメータは再送信と再試行間隔です。

APの再送信間隔と再試行間隔は、グローバルレベルとAPレベルの両方で設定できます。グローバル設定では、これらの設定パラメータがすべてのAPに適用されます。つまり、再送信間隔とリトライ回数は、すべてのAPで同じです。

WLCからの問題のあるログ：

```
*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
*spamApTask6: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1
-Traceback:  0xe69bba3a5f 0xe69b9b9446 0xe69bdc5e3b 0xe69b8f238c 0xe69bbaf33b 0xe69cc8041b 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d
*spamReceiveTask: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:
-Traceback:  0xe69bba3a5f 0xe69b981950 0xe69b76dd5c 0xe69cc757c2 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d
*spamApTask5: Jun 01 17:17:55.424: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7521 1c:d1:e0:43:1d:20:  DTLS connection closed forAP
*spamApTask5: Jun 01 17:17:55.423: %CAPWAP-3-MAX_RETRANSMISSIONS_REACHED: capwap_ac_sm.c:8073 Max retransmissions reached on
),number of pending messages(2)
```

解決策：問題がすべてのサイトで発生する場合は、ワイヤレスのグローバル設定で**Retransmit count** および**Retransmit interval** を大きくします。すべてのAPに問題がある場合に値を増やすオプション。



グローバルコンフィギュレーションでAP再送信設定パラメータを変更するオプション

問題が1つのリモートサイトに特有のものである場合は、特定のAPで**Retransmit count** および**Retransmit interval**を増やすと問題が解決します。

特定のAPでAP再送信設定パラメータを変更するオプション

使用例 4

APとWLCの関連付けが完全に解除され、コントローラに再接続できなくなります。デジタル証明書に関連している可能性があります。

Cisco WLCとAPに関するデバイス証明書の概要は次のとおりです。

- シスコから提供されるすべてのデバイスには、デフォルトで10年の有効期間を持つ証明書が付属します。
- この証明書は、Cisco WLCとAPの間の認証に使用されます。
- 証明書を使用して、APとWLCはセキュアなDatagram Transport Layer Security(DTLS)トンネルを確立します。

証明書に関連して、次の2種類の問題が発生しました。

問題1：古いAP（WLCに加入したくない）。

APへのコンソール接続は、問題の判別に役立ち、ログは次のようになります。

```
*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：新しいAPは古いWLCに加入したくない。
APへのコンソールには、次のようなエラーが表示されます。

```
[*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

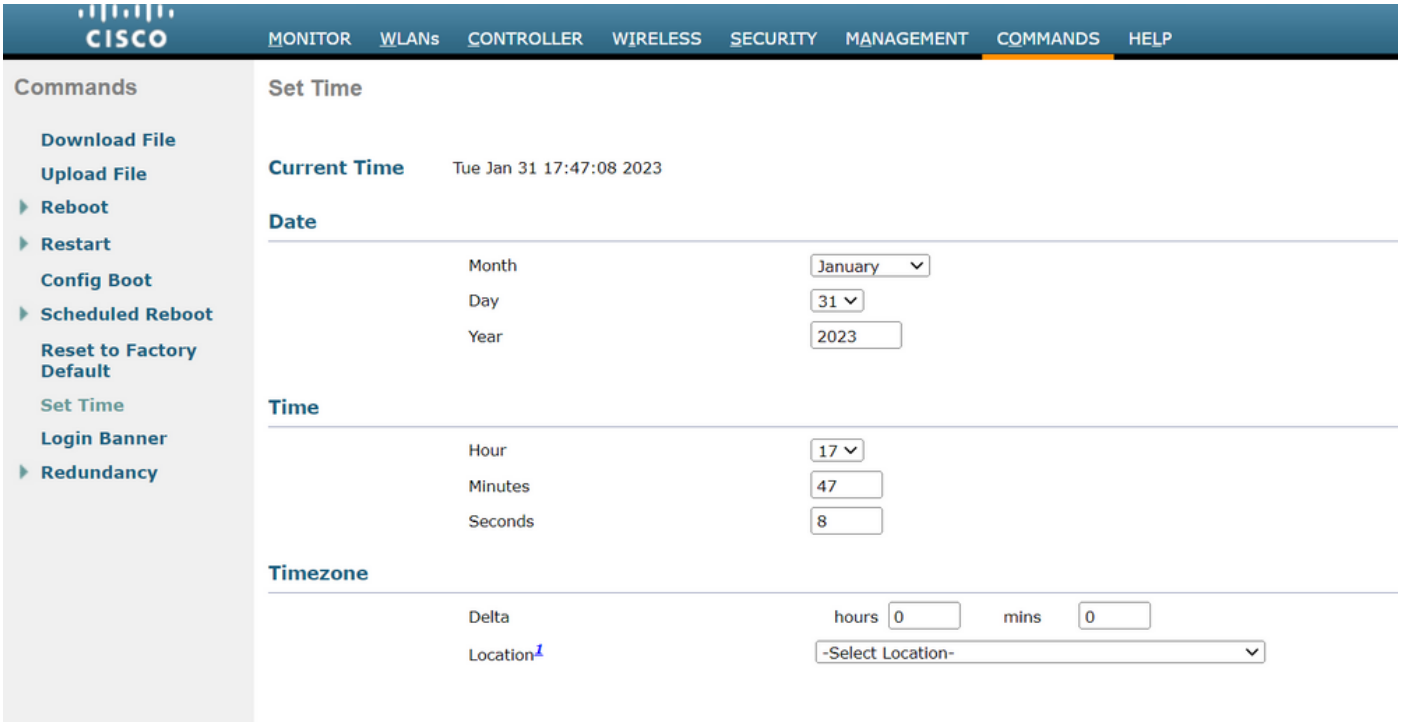
ソリューション：

1. NTPはCLIを使用して手動で時刻を無効化および設定します。

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

2. NTPは、GUIを使用して手動で時刻を無効化および設定します。

表示されているNTPサーバを削除するには、**Controller** > **NTP** > **Server** > **Commands** > **Set Time**に移動します。



GUIで手動で時刻を設定する場所

2. コントローラの製造元でインストールされた証明書(MIC)を無効にします。このコマンドは、最新バージョンでのみ受け入れられます。

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

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。