ワイヤレスLANコントローラ(WLC)でのID PSKのトラブルシューティング

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[アイデンティティPSKのフローについて](#)
[トラブルシューティングシナリオ](#)
[シナリオ1.クライアントが正常に接続するシナリオの通過](#)
[シナリオ2：クライアントが誤ったパスワードで接続を試みる](#)
[シナリオ3:Radiusサーバに到達できない](#)
[シナリオ4. RADIUSサーバから送信された誤った上書きパラメータ](#)
[シナリオ5. RADIUSサーバでクライアントポリシーが設定されていない](#)

概要

このドキュメントでは、Cisco Wireless LAN Controller(WLC)でのID事前共有キー(PSK)接続の問題をトラブルシューティングする方法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。

- コード8.5以降およびIdentity Services Engine(ISE)を実行するCisco WLC
- 中央でスイッチングされるWLAN（ID PSKを使用したFlexConnectローカルスイッチングは現在サポートされていません）
- WLCおよびISEでのアイデンティティPSK設定。これは、次のリンクで確認できます。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアリリース8.5.103.0が稼働するCisco 5508シリーズWLC
- バージョン2.2が稼働するCisco ISE

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的

な影響について確実に理解しておく必要があります。

アイデンティティPSKのフローについて

ステップ1：クライアントは、PSK+MAC認証が有効になっているService Set Identifier(SSID)に関連付け要求を送信します。

ステップ2:MAC認証でWLCのコンタクトが有効になっているため、RADIUSサーバはクライアントのMACアドレスを確認します。

ステップ3:Radiusサーバはクライアントの詳細を確認し、使用する認証タイプとしてPSKを指定するCisco avペアと、クライアントに使用するキー値を送信します。

ステップ4：これが受信されると、WLCはクライアントにアソシエーション応答を送信します。WLCとRADIUSサーバの間の通信に遅延が発生した場合、クライアントはアソシエーションループに陥り、RADIUSサーバから応答を受信する前に2番目のアソシエーション要求を送信する可能性があるため、この手順を認識することが重要です。

ステップ 5： WLCは、PMKキーとしてradiusサーバから送信されたキー値を使用します。次に、アクセスポイント(AP)は4ウェイハンドシェイクを続行し、クライアントに設定されたパスワードがRADIUSサーバから送信された値と一致することを確認します。

ステップ6：クライアントはDHCPプロセスを完了し、RUN状態に移行します。

トラブルシューティングシナリオ

Identity PSKの問題をトラブルシューティングするには、次のデバッグが必要です。

WLCでのデバッグ：

- **debug client client_mac。ここで、client_macはクライアントの**テストのMACアドレスです。
- **debug aaa detail enable**

シナリオ1.クライアントが正常に接続するシナリオの通過

クライアントはアソシエーション要求をAPに送信します。

```
*apfMsConnTask_6: Sep 21 15:01:43.496: e8:50:8b:64:4f:45 Association received from mobile on
BSSID 28:6f:7f:e2:24:cf AP AP_2802-1
```

次に、WLCがRADIUSサーバに接続して、クライアントのMACアドレスを確認します。

```
*aaaQueueReader: Sep 21 15:01:43.498: AuthenticationRequest: 0x2b8c8a9c
*apfMsConnTask_6: Sep 21 15:01:43.498: e8:50:8b:64:4f:45 apfProcessAssocReq (apf_80211.c:11440)
Changing state for mobile e8:50:8b:64:4f:45 on AP 28:6f:7f:e2:24:c0 from Associated to AAA
Pending

*aaaQueueReader: Sep 21 15:01:43.498:
Callback.....................................0x10762018
```

```
*aaaQueueReader: Sep 21 15:01:43.498:
protocolType.............................0x40000001
```

radiusサーバは、認証に使用されるPSK方式タイプとキーも含むAccess-Acceptメッセージで応答します。

```
*radiusTransportThread: Sep 21 15:01:43.794: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 21 15:01:43.794:
structureSize............................313

*radiusTransportThread: Sep 21 15:01:43.794:
resultCode...............................0


*radiusTransportThread: Sep 21 15:01:43.794:         Packet contains 5 AVPs:

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[01] User-
Name.............................E8-50-8B-64-4F-45 (17 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[02]
State................................ReauthSession:0a6a20770000000059c346ed (38 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[03]
Class................................CACS:0a6a20770000000059c346ed:ISE/291984633/6 (45
bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[04] Cisco / PSK-
Mode.....................ascii (5 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[05] Cisco /
PSK............................cisco123 (8 bytes)
```

これを受信すると、WLCがアソシエーション応答を送信し、4ウェイハンドシェイクが発生することがわかります。

```
*apfReceiveTask: Sep 21 15:01:43.924: e8:50:8b:64:4f:45 Sending assoc-resp with status 0
station:e8:50:8b:64:4f:45 AP:28:6f:7f:e2:24:c0-01 on apVapId 1
```

4ウェイハンドシェイク：

```
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.994: e8:50:8b:64:4f:45 Sending EAPOL-Key Message to mobile
e8:50:8b:64:4f:45
   state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.998: e8:50:8b:64:4f:45 Received EAPOL-key in PTK_START
state (message 2) from mobile e8:50:8b:64:4f:45
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.998: e8:50:8b:64:4f:45 Received valid MIC in EAPOL Key
Message M2!!!!!
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.999: e8:50:8b:64:4f:45 Sending EAPOL-Key Message to mobile
e8:50:8b:64:4f:45
   state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_5: Sep 21 15:01:44.003: e8:50:8b:64:4f:45 Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile e8:50:8b:64:4f:45
```

これが完了すると、クライアントはDHCPプロセスを完了し、RUN状態になります（重要なセクションを示すために出力がクリップされます）。

```
(WLC_1) >show client detail e8:50:8b:64:4f:45
Client MAC Address..............................  e8:50:8b:64:4f:45
Client Username ................................  E8-50-8B-64-4F-45
Hostname: ......................................  S6-edge
Device Type: ...................................  Android-Samsung-Galaxy-Phone
AP MAC Address..................................  28:6f:7f:e2:24:c0
AP Name.........................................  AP_2802-1
Wireless LAN Network Name (SSID)................  Identity PSK
Wireless LAN Profile Name.......................  Identity PSK
Security Policy Completed.......................  Yes
Policy Manager State............................  RUN
```

シナリオ2：クライアントが誤ったパスワードで接続を試みる

ステップの最初のシーケンスは、渡された認証と同じままです。

- クライアントがアソシエーション要求を送信します。
- WLCはこれを受信すると、RADIUSサーバとの通信を開始して、クライアントのMACアドレスを確認します。
- RADIUSサーバにクライアントの詳細がある場合、PSKであるキー値と認証タイプを使用してaccess-acceptを送信します。
- 障害が認識される有用なセクションは、4ウェイハンドシェイクです。

APはメッセージ1を送信し、クライアントはメッセージ2で応答します。

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.661: 50:8f:4c:9d:ef:87 Received EAPOL-key in PTK_START
state (message 2) from mobile 50:8f:4c:9d:ef:87
```

ただし、PMKキーの値（パスワード）が異なるため、APとクライアントは異なるキーを取得し、メッセージ2で無効なMIC受信が発生します。

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.662: 50:8f:4c:9d:ef:87 Received EAPOL-key M2 with invalid
MIC from mobile 50:8f:4c:9d:ef:87 version 2
*osapiBsnTimer: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 802.1x 'timeoutEvt' Timer expired for
station 50:8f:4c:9d:ef:87 and for message = M2
*Dot1x_NW_MsgTask_7: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 Retransmit 1 of EAPOL-Key M1 (length
121) for mobile 50:8f:4c:9d:ef:87

The client then is then de-authenticated by the WLC:
*Dot1x_NW_MsgTask_7: Sep 21 15:12:50.825: 50:8f:4c:9d:ef:87 Sent Deauthenticate to mobile on
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)

<noscript>
```

もう1つの便利な出力は、「show client detail」です。 次に、クライアントがSTART状態のままになっていることを示します。

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.662: 50:8f:4c:9d:ef:87 Received EAPOL-key M2 with invalid
MIC from mobile 50:8f:4c:9d:ef:87 version 2
*osapiBsnTimer: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 802.1x 'timeoutEvt' Timer expired for
station 50:8f:4c:9d:ef:87 and for message = M2
*Dot1x_NW_MsgTask_7: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 Retransmit 1 of EAPOL-Key M1 (length
121) for mobile 50:8f:4c:9d:ef:87

The client will then be de-authenticated by the WLC:
*Dot1x_NW_MsgTask_7: Sep 21 15:12:50.825: 50:8f:4c:9d:ef:87 Sent Deauthenticate to mobile on
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)
```

シナリオ3:Radiusサーバに到達できない

WLCは、アソシエーション要求を受信すると、RADIUSサーバへの接続を試行します。RADIUSサーバに到達できない場合、WLCは（再試行回数に達するまで）RADIUSサーバへの接続を繰り返し試行します。 RADIUSサーバが設定された再試行回数（デフォルト値は5）の後に到達不能であることが検出されると、WLCは次に示すようにステータスコード1のアソシエーション応答を送信します。

```
*apfReceiveTask: Sep 21 15:28:55.777: 50:8f:4c:9d:ef:87 Sending assoc-resp with status 1
station:50:8f:4c:9d:ef:87 AP:a0:e0:af:62:f3:c0-00 on apVapId 1
*apfReceiveTask: Sep 21 15:28:55.777: 50:8f:4c:9d:ef:87 Sending Assoc Response (status:
'unspecified failure') to station on AP AP_2802-2 on BSSID a0:e0:af:62:f3:c0 ApVapId 1 Slot 0,
mobility role 0
```

RADIUSサーバの統計情報で増加する再試行要求とタイムアウト要求の数を確認することもできます。この場合は、次の図に示すように**[Monitor] > [Statistics] > [RADIUS Servers]に移動できます。**

シナリオ4. RADIUSサーバから送信された誤った上書きパラメータ

PSKとキーとともにプッシュできるパラメータがいくつかあります。たとえば、VLAN、ACL、ユーザロールなどです。ただし、RADIUSサーバから送信されたACLエントリが設定されていない場合、RADIUSサーバが認証要求を承認しても、WLCはクライアントを拒否します。これは、クライアントのデバッグで明確に確認できます。

```
*radiusTransportThread: Sep 22 14:39:05.499: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 22 14:39:05.499:
structureSize.............................376

*radiusTransportThread: Sep 22 14:39:05.499:
resultCode.................................0

*radiusTransportThread: Sep 22 14:39:05.499:
protocolUsed.............................0x00000001

*radiusTransportThread: Sep 22 14:39:05.499:         Packet contains 7 AVPs:

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[01] User-
Name..............................E8-50-8B-64-4F-45 (17 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[02]
State..................................ReauthSession:0a6a20770000002659c493e9 (38 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[03]
Class..................................CACS:0a6a20770000002659c493e9:ISE/291984633/78 (46
bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[04] Cisco / PSK-
Mode.......................ascii (5 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[05] Cisco /
PSK............................cisco123 (8 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[06] Unknown Cisco / Attribute
19............teacher (7 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[07] Airespace / ACL-
Name...................testing (7 bytes)
```

クライアントのデバッグ:

```
*apfReceiveTask: Sep 22 14:39:05.564: e8:50:8b:64:4f:45  ACL received from RADIUS does not exist
in WLC de-authenticating the client
*apfReceiveTask: Sep 22 14:39:05.628: e8:50:8b:64:4f:45 Sending assoc-resp with status 12
station:e8:50:8b:64:4f:45 AP:28:6f:7f:e2:24:c0-01 on apVapId 1
```

シナリオ5. RADIUSサーバでクライアントポリシーが設定されていない

RADIUSサーバに到達可能で、クライアントのRADIUSサーバにポリシーが設定されていない場合、WLANでグローバルに設定されたPSKを使用している場合にのみ接続できます。他のエントリは失敗します。アクティブなグローバルPSK認証とアクティブなID PSK認証を区別する特別な点は、プッシュされる上書きパラメータがないdebug Authentication, Authorization, and Accounting（AAA；認証、認可、アカウンティング）の出力に限られます。

```
*radiusTransportThread: Sep 22 14:32:13.734: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 22 14:32:13.734:
structureSize.............................269

*radiusTransportThread: Sep 22 14:32:13.734:
resultCode.................................0
```

```
*radiusTransportThread: Sep 22 14:32:13.734:
protocolUsed.............................0x00000001

*radiusTransportThread: Sep 22 14:32:13.734:
proxyState...............................50:8F:4C:9D:EF:87-00:00

*radiusTransportThread: Sep 22 14:32:13.734:         Packet contains 3 AVPs:

*radiusTransportThread: Sep 22 14:32:13.734:             AVP[01] User-
Name.............................50-8F-4C-9D-EF-87 (17 bytes)

*radiusTransportThread: Sep 22 14:32:13.734:             AVP[02]
State................................ReauthSession:0a6a20770000002359c49240 (38 bytes)

*radiusTransportThread: Sep 22 14:32:13.734:             AVP[03]
Class................................CACS:0a6a20770000002359c49240:ISE/291984633/74 (46
bytes)
```