ワイヤレス LAN コントローラの識別 PSK を解決して下さい

目次

概要

この資料に Ciscoワイヤレス LAN コントローラ（WLC）の識別事前共有キー（PSK）接続に関する問題を解決する方法を記述されています。

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 およびより高いおよび Identity Services Engine （ISE）を実行する Cisco WLC。
- WLC および ISE の識別 PSK 設定。 これはこのリンクで見つけることができます:

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くものです。

- ソフトウェア リリース 8.5.103.0 を実行する Cisco 5508 シリーズ WLC。
- バージョン 2.2 を実行する 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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

識別 PSK のフローを理解して下さい

ステップ 1.クライアントは PSK+MAC 認証と有効に なる Service Set Identifier （ SSID ）に Association 要求を送信 します。

呼び出します。 MAC 認証が WLC 連絡先を有効に したので、RADIUSサーバはクライアントの MAC アドレスを確認することです。

ステップ 3. RADIUSサーバはクライアント 詳細を確認し、PSK をと同時に使用されるべき認証種別、またクライアントに使用するべきキー値 規定 する Cisco AVペアを送信します。

ステップ 4 これが受け取られれば WLC はクライアントへのアソシエーション応答を返します。WLC と RADIUSサーバ間のコミュニケーションに遅延があるようにこのステップに気づいていることは重要、クライアント応答が RADIUSサーバから届く前にそれらが第 2 Association 要求を送信 する アソシエーション ループにはまり込むことができますです。

ステップ 5 WLC は RADIUSサーバによって送信 される マスタ鍵としてキー値を使用します。Access Point （ AP ）は確認する四方ハンドシェイクをそれからクライアントで設定されるパスワードは RADIUSサーバによって送信 される値とマッチすることを続行します。

ステップ 6 クライアントはそして DHCPプロセスを完了し、走行状態に同様に移動します。

シナリオを解決して下さい

これらのデバッグが識別 PSK 問題を解決するために必要となります:

WLC のデバッグ:

- クライアント_mac がクライアントのテストの MAC アドレスであるところ、**デバッグ クライアント client_mac。**
- **debug aaa detail enable**

クライアントが上手く接続するところシナリオ 1.パス シナリオ

クライアントは AP に Association 要求を送信 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
```

WLC はそれからクライアントのMACアドレスを確認するために RADIUSサーバを接続します:

```
*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サーバはまた認証のために使用されるキーおよび PSK メソッドの型が含まれている

Access-Accept メッセージと応答します:

```
*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)
```

これが受け取られれば WLC がアソシエーション応答を返し、四方ハンドシェイクが起こ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
```

四方ハンドシェイク:

```
*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
```

これがされれば、クライアントは DHCPプロセスを完了し、走行状態に入ります (重要なセクションを示すために出力は切られます) :

```
(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.クライアントは不適切なパスワードで接続することを試みます

ステップの最初 の シーケンスは取得された認証のそれと同じをとどまります。

- クライアントは Association 要求を送信 します。
- WLC がこれを受け取れば、クライアントのMACアドレスを確認するために RADIUSサーバが付いている通信を始めます。
- RADIUSサーバが持っていればクライアントはそれを送信 します PSK であるキー値および認証種別との access-accept を詳述します。
- 失敗が注意することができる有用なセクションは四方ハンドシェイクにあります。

AP はクライアントがメッセージ 2 と応答するメッセージ 1 を送信 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、 (パスワード) メッセージ 2 の無効 MIC 受信という結果に終る AP およびクライアントを得ます異なるキーを評価します別のマスタ鍵が原因で:

```
*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)
```

チェックするべきもう一つの有用な出力は「示しますクライアント 詳細」をです。 クライアントが開始する状態のままになっていることを見ることができます:

```
*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)
```

到達不能 シナリオ 3. RADIUSサーバ

WLC は Association 要求を受け取れば RADIUSサーバを接続することを試みます。 RADIUSサーバが到達不能なら、WLC は繰り返し (リトライ回数が達するまで) RADIUSサーバを接続することを試みます。 RADIUSサーバがリトライの設定された番号の後で到達不能であるために (検出する デフォルト値はここに示されているように 5) WLC 返しますステータス スコード 1 のアソシエーション応答をです:

```
*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
```

またイメージに示すように **>Statistics >RADIUS サーバを監視するために**ナビゲートできる RADIUSサーバ統計情報で増加する再試行要求およびタイムアウト 要求の数を表示できます:

シナリオ 4. RADIUSサーバによって送信 される不正確な上書きする パラメータ

VLAN、ACL およびユーザの役割のような PSK およびキーと共に、押すことができる複数のパラメータがあります。 ただし、RADIUSサーバによって送信 される ACL項目がそれから設定されなければ WLC は RADIUSサーバが認証要求を承認しても、クライアントを拒否します。 これはクライアント デバッグではっきりわかる場合があります:

```
*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 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
```

RADIUSサーバで設定されないシナリオ 5.クライアント ポリシー

RADIUSサーバは到達可能のが、クライアントのための RADIUSサーバで設定されるポリシーがないとき PSK を使用するときだけ、WLAN の下でグローバルに設定されて接続されることができます。 他のどのエントリも失敗します。 特定の何もはたらくグローバル な PSK 認証および debug authentication のを除くはたらく識別 PSK 認証、許可、および (AAA) 出力される上書きする パラメータがない説明を区別するためにありません押される:

```
*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)
```