无线LAN控制器上的身份PSK故障排除

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[了解身份PSK的流程](#)
[故障排除方案](#)
[场景1.传递客户端成功连接的场景](#)
[场景2.客户端尝试使用不正确的密码连接](#)
[场景3. RADIUS服务器无法访问](#)
[场景4. RADIUS服务器发送的覆盖参数不正确](#)
[场景5.未在RADIUS服务器上配置客户端策略](#)

简介

本文档介绍如何排除思科无线局域网控制器(WLC)上的身份预共享密钥(PSK)连接问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 运行代码8.5及更高版本和身份服务引擎(ISE)的Cisco WLC
- 集中交换WLAN（当前不支持带身份PSK的FlexConnect本地交换）
- WLC和ISE上的身份PSK配置。此链接中可以找到：

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

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.5.103.0的Cisco 5508系列WLC
- 运行版本2.2的思科ISE

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

了解身份PSK的流程

步骤1.客户端向启用PSK+MAC身份验证的服务集标识符(SSID)发送关联请求。

步骤2.由于MAC身份验证已启用WLC联系人，RADIUS服务器将验证客户端的MAC地址。

步骤3. Radius服务器验证客户端详细信息并发送Cisco av-pairs，它指定PSK作为要使用的身份验证类型以及要用于客户端的密钥值。

步骤4.收到此消息后，WLC将关联响应发送到客户端。必须了解此步骤，因为WLC和radius服务器之间的通信存在延迟，客户端可能陷入关联环路，在该环路中，客户端在从radius服务器接收响应之前发送第二个关联请求。

第五步： WLC使用RADIUS服务器发送的密钥值作为PMK密钥。接着，接入点(AP)继续进行四次握手，验证客户端上配置的密码是否与RADIUS服务器发送的值匹配。

步骤6.然后客户端完成DHCP过程并进入RUN状态。

故障排除方案

排除Identity PSK问题时，需要执行以下调试：

WLC上的调试：

- **debug client client_mac，**其中**client _mac**是客户端测试的MAC地址。
- **debug aaa detail enable**

场景1.传递客户端成功连接的场景

客户端向AP发送关联请求：

```
*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
```

然后，WLC与RADIUS服务器联系以验证客户端MAC地址：

```
*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服务器以Access-Accept消息响应，该消息还包含用于身份验证的PSK方法类型和密钥：

```
*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)
```

收到此消息后，您可以看到WLC发送关联响应，并发生四次握手：

```
*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
```

四次握手：

```
*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
```

完成此操作后，客户端完成DHCP进程并进入RUN状态（输出被截断以显示重要部分）：

```
(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
```

场景2.客户端尝试使用不正确的密码连接

步骤的初始顺序与通过的身份验证的顺序相同。

- 客户端发送关联请求。
- WLC收到此消息后，会启动与RADIUS服务器的通信以验证客户端MAC地址。
- 如果RADIUS服务器具有客户端详细信息，它会发送一个带有密钥值和身份验证类型（即PSK）的access-accept。
- 可注意到故障的有用部分是四次握手。

AP发送消息1，客户端向其回复消息2:

```
*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
```

但是，由于PMK密钥值（密码）不同，AP和客户端派生不同的密钥，从而导致消息2中的MIC接收无效：

```
*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>
```

另一个有用的输出是“show client detail”。 在此您可以看到客户端停滞在START状态：

```
*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)
```

场景3. RADIUS服务器无法访问

WLC在收到关联请求后尝试与RADIUS服务器联系。如果RADIUS服务器无法访问，WLC会反复尝试与RADIUS服务器联系（直到达到重试计数为止）。 一旦在配置的重试次数（默认值为5）后检测到radius服务器无法访问，WLC将发送状态代码为1的关联响应，如下所示：

```
*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
```

您还可以看到radius服务器统计信息中增加的重试请求和超时请求数，您可以导航到**Monitor > Statistics > RADIUS Servers**，如图所示：

场景4. RADIUS服务器发送的覆盖参数不正确

PSK和密钥可以同时推送多个参数，例如VLAN、ACL和用户角色。但是，如果RADIUS服务器发送的ACL条目未配置，则WLC会拒绝客户端，即使RADIUS服务器批准身份验证请求也是如此。在客户端调试中可以清楚地看到：

```
*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)
```

客户端调试:

```
*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
```

场景5.未在RADIUS服务器上配置客户端策略

当RADIUS服务器可访问，但客户端的RADIUS服务器上没有配置策略时，只有使用PSK（在WLAN下全局配置），它才能连接。任何其他条目都会失败。除了调试身份验证、授权和记帐(AAA)输出中没有推送的任何覆盖参数，没有特定于区分工作全局PSK身份验证和工作身份PSK身份验证的内容：

```
*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)
```