

排除在无线局域网控制器的身份PSK故障

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[了解身份PSK流](#)

[排除方案故障](#)

[方案1.通行证方案客户端成功的地方连接](#)

[方案2.客户端设法连接不正确的密码](#)

[不可得到方案3.的RADIUS服务器](#)

[RADIUS服务器发送的方案4.不正确覆盖参数](#)

[方案5.在RADIUS服务器没配置的客户端策略](#)

Introduction

本文描述如何排除身份预共享密钥(PSK)在Cisco无线LAN控制器(WLC)的连接问题故障。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 运行代码8.5及以后和身份服务引擎的Cisco WLC (ISE)
- 在中央转换WLAN (当前不支持与身份PSK的FlexConnect本地交换)
- 身份在WLC和ISE的PSK配置。这可以在此链路找到：

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

Components Used

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Cisco ISE

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

了解身份PSK流

步骤1.客户端发送一关联申请到服务集标识(SSID)启用PSK+MAC认证。

Step 2.因为MAC验证启用了WLC联系，RADIUS服务器是验证客户端的MAC地址。

步骤3. RADIUS服务器验证客户端详细资料并且发送指定PSK的Cisco AV对，当认证类型将使用的以及将用于客户端关键值。

第4.步。一旦这被接受WLC发送对客户端的关联回应。知道此步骤，好象通信的延迟WLC和RADIUS服务器之间是重要的，客户端能陷在关联循环，他们发送秒钟关联申请，在答复从RADIUS服务器前被收到。

第5.步。WLC使用RADIUS服务器发送的关键值作为万能密钥。接入点(AP)然后继续进行验证的四种方式的握手在客户端配置的密码匹配RADIUS服务器发送的值。

第6.步。客户端然后完成DHCP进程并且搬入运转状态。

排除方案故障

要求这些调试排除身份PSK问题故障：

在WLC的调试：

- 调试客户端client_mac，其中客户端_mac是客户端的测试的MAC地址。
- debug aaa detail enable

方案1.通行证方案客户端成功的地方连接

客户端发送关联申请到AP：

```
*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然后联系RADIUS服务器验证客户端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服务器回应也包含PSK方法类型和键使用认证的Access-Accept消息：

```
*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:0a6a2077000000059c346ed (38 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:          AVP[03]
Class.....CACS:0a6a2077000000059c346ed: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)

```

一旦这被接受您能看到WLC发送关联回应，并且四种方式的握手发生：

```

*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

```

四种方式的握手：

```

*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

```

一旦这执行，客户端完成DHCP进程并且进入运转状态(输出截去显示重要部分)：

```

(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

```

方案2.客户端设法连接不正确的密码

步骤初始顺序坚持同那一个被通过的认证一样。

- 客户端发送一关联申请。
- 一旦WLC接受此，启动通信以RADIUS服务器验证客户端MAC地址。
- 如果RADIUS服务器有客户端选派它发送与是PSK的关键值和认证类型的一access-accept。
- 故障可以被注意的有用的部分在四种方式的握手。

AP传送信息1，客户端回应消息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
```

然而，由于另外万能密钥重视(密码)导致在消息2的一个无效MIC收据的AP和客户端派生不同的键：

```
*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>

检查的另一个有用的输出是‘显示客户端详细资料’。您能看到客户端在启动状态被滞留：

```
*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)
```

不可得到方案3.的RADIUS服务器

一旦接受关联申请，WLC设法联系RADIUS服务器。万一RADIUS服务器是不可得到的，WLC重复设法联系RADIUS服务器(直到重试计数被到达)。一旦发现RADIUS服务器是不可得到的在重试次数以后的配置的号码(DEFAULT值是5)WLC发送与状态码1的一种关联回应如显示这里：

```
*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
```

您能也看到重试次数请求和超时的编号请求哪些在RADIUS服务器统计数据增长，如镜像所显示，您能连接[监控>统计数据>RADIUS服务器](#)：

Monitor

Summary

▶ Access Points

▶ Cisco CleanAir

▼ Statistics

Controller

AP Join

Ports

RADIUS Servers

Mobility Statistics

IPv6 Neighbor Bind

Counters

PMIPv6 LMA Statistics

Preferred Mode

Optimized Roaming

▶ CDP

▶ Rogues

Clients

Sleeping Clients

Multicast

▶ Applications

▶ Lync

Local Profiling

RADIUS Servers > Authentication Stats

Server Index	2
Server Address	10.1.1.1
Admin Status	Enabled

Authentication Server Statistics

Msg Round Trip Time (milliseconds)	0
First Requests	8
Retry Requests	33
Accept Responses	0
Reject Responses	0
Challenge Responses	0
Malformed Messages	0
Bad Authenticator Msgs	0
Pending Requests	0
Timeout Requests	39
Unknown Type Msgs	0
Other Drops	0

RADIUS服务器发送的方案4.不正确覆盖参数

有可以与PSK和键一起被推进，例如VLAN、ACL和用户角色的几个参数。然而，如果然后没有配置RADIUS服务器发送的ACL条目WLC拒绝客户端，即使RADIUS服务器审批认证请求。这在客户端调试能清楚看见：

```
*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

```

方案5.在RADIUS服务器没配置的客户策略

当RADIUS服务器可及时的，但是没有在客户端的RADIUS服务器配置的策略，能得到连接，只有当使用PSK，配置全局在WLAN下。所有其他条目将发生故障。特定的没什么区分在一个工作的全局PSK认证和一个工作的身份PSK认证除了在debug authentication，不会有任何覆盖参数被推进(AAA)输出之间的授权和认为：

```

*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:0a6a2077000002359c49240 (38 bytes)

*radiusTransportThread: Sep 22 14:32:13.734: AVP[03]
Class.....CACS:0a6a2077000002359c49240:ISE/291984633/74 (46
bytes)