调试身份验证

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[捕获调试](#)
[EAP](#)
[MAC 验证](#)
[WPA](#)
[管理/HTTP 身份验证](#)
[相关信息](#)

简介

无线通信以许多方式使用身份验证。最常见的身份验证类型是不同类型和形式的可扩展的身份验证协议 (EAP)。其他身份验证类型包括 MAC 地址身份验证和管理身份验证。本文档介绍如何调试和解释调试身份验证的输出。排查无线安装故障时，这些调试的信息非常重要。

注意：本文档中涉及非思科产品的部分基于作者的经验，而非正式培训。它们旨在为您提供便利，而不是提供技术支持。若要获得非思科产品的权威技术支持，请与该产品的技术支持人员联系。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份验证，因为它与无线网络相关
- 思科 IOS® 软件命令行界面 (CLI)
- RADIUS 服务器配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 基于 Cisco IOS 软件的、任何型号和版本的无线产品
- Hilgraeve HyperTerminal

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

捕获调试

如果不能捕获和分析调试信息，则信息毫无用处。捕获此数据的最简单方法是使用在 Telnet 或通信应用程序中内置的屏幕捕获功能。

以下示例说明如何使用 Hilgraeve HyperTerminal 应用程序捕获输出。大多数 Microsoft Windows 操作系统都包含 HyperTerminal，但是您可以将概念应用于任何终端仿真应用程序。有关该应用程序的更完整信息，请参阅 Hilgraeve 。

完成以下步骤，以将 HyperTerminal 配置为与接入点 (AP) 或桥进行通信：

1. 要打开 HyperTerminal，请选择“开始”>“程序”>“系统工具”>“通信”>“HyperTerminal”。

   图 1 – HyperTerminal 启动

2. HyperTerminal 打开后，完成以下步骤：

   a. 输入连接的名称。

   b. 选择图标。

   c. Click OK.

3. 对于 Telnet 连接，完成以下步骤：

   a. 从“Connect Using”下拉菜单中，选择 TCP/IP。

   b. 输入要在其中运行调试的设备的 IP 地址。

   c. Click OK.

      图 2 – Telnet 连接

4. 对于控制台连接，完成以下步骤：

   a. 从“Connect Using”下拉菜单中，选择要连接控制台电缆的 COM 端口。

   b. Click OK.

      将显示连接的属性表。

   c. 设置与控制台端口的连接的速度。

d. 要恢复默认端口设置，请单击 Restore Defaults。

注意：大多数思科产品都采用默认端口设置。

默认端口设置为：

- Bits per second — 9600
- Data bits — 8
- 奇偶校验 - 无
- 停止位 — 1
- Flow control — None

图 3 – COM1 属性

此时，将建立 Telnet 或控制台连接，并且提示您输入用户名和密码。

注意：Cisco Aironet设备分配默认用户名和密码Cisco（区分大小写）。

5. 要运行调试，请完成以下步骤：

a. 发出 enable 命令以进入特权模式。

b. 输入启用密码。

注意：请记住，Aironet设备的默认密码是Cisco（区分大小写）。

注意：要查看Telnet会话的调试输出，请使用terminal monitor或term mon命令打开终端监视器。

图 4 – 连接的 Telnet 会话

6. 建立连接后，完成以下步骤以收集屏幕捕获：

a. 从“Transfer”菜单中选择 Capture Text。

图 5 – 保存屏幕捕获

b. 提示您为输出输入文件名的对话框打开时，输入文件名。

7. 完成以下步骤以禁用屏幕换行：

注意：禁用屏幕绕排时，可以更轻松地读取调试。

a. 从 HyperTerminal 菜单中，选择 File。

b. 选择属性。

c. 在连接属性表上，单击 Settings 选项卡。

d. 单击 ASCII Setup。

e. 取消选中 Wrap lines that exceed terminal width。

f. 要关闭“ASCII Settings”，请单击 OK。

g. 要关闭连接属性表，请单击 OK。

图 6 – ASCII Settings

现在可以将任何屏幕输出捕获为文本文件，运行的调试取决于协商的内容。本文档接下来的部分介绍调试提供的协商连接的类型。

EAP

以下调试对于 EAP 身份验证非常有帮助：

- debug radius authentication — 此调试的输出以下面的词开头：RADIUS.
- debug dot11 aaa authenticator process — 此调试的输出以下面的文本开头：dot11_auth_dot1x_。
- debug dot11 aaa authenticator state-machine — 此调试的输出以下面的文本开头：dot11_auth_dot1x_run_rfsm。

这些调试显示：

- 在身份验证对话框的 RADIUS 部分期间报告的内容
- 在该身份验证对话框期间采取的操作
- 身份验证对话框在其中转换的各种状态

以下示例显示成功的轻量 EAP (LEAP) 身份验证：

成功的 EAP 身份验证示例
<#root> Apr 8 17:45:48.208: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start Apr 8 17:45:48.208: dot11_auth_dot1x_send_id_req_to_client: *sending identity request for 0002.8aa6.304f* Apr 8 17:45:48.208: dot11_auth_dot1x_send_id_req_to_client: Started timer client_timeout 30 seconds Apr 8 17:45:48.210: dot11_auth_parse_client_pak: Received EAPOL packet from 0002.8aa6.304f Apr 8 17:45:48.210: dot11_auth_dot1x_run_rfsm: Executing Action(**CLIENT_WAIT,EAP_START**) for 0002.8aa6.304f Apr 8 17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:

```
    sending identity request for 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr  8 17:45:48.212: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.212: dot11_auth_parse_client_pak:
    id is not matching req-id:1resp-id:2, waiting for response
Apr  8 17:45:48.213: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.213: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 17:45:48.214: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.214: dot11_auth_dot1x_send_response_to_server:
    tarted timer server_timeout 60 seconds
Apr  8 17:45:48.214: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.214: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:45:48.215: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.215: RADIUS(0000001C): Storing nasport 17 in rad_db
Apr  8 17:45:48.215: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.215: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.216: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.216: RADIUS(0000001C): sending
Apr  8 17:45:48.216: RADIUS(0000001C): Send Access-Request
    to 10.0.0.3:1645 id 21645/93, len 139
Apr  8 17:45:48.216: RADIUS:  authenticator 92 26 A8 31 ED 60 6A 88
    - 84 8C 80 B2 B8 26 4C 04
Apr  8 17:45:48.216: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.216: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.217: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.217: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.217: RADIUS:  Service-Type        [6]   6   Login  [1]
Apr  8 17:45:48.217: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.217: RADIUS:  EAP-Message         [79]  14
Apr  8 17:45:48.218: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
    [?????aironet]
Apr  8 17:45:48.218: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless     [19]
Apr  8 17:45:48.218: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.218: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.218: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.224: RADIUS: Received from id 21645/93 10.0.0.3:1645,
    Access-Challenge, len 69
Apr  8 17:45:48.224: RADIUS:  authenticator C8 6D 9B B3 67 60 44 29
    - CC AB 39 DE 00 A9 A8 CA
Apr  8 17:45:48.224: RADIUS:  EAP-Message         [79]  25
Apr  8 17:45:48.224: RADIUS:   01 43 00 17 11 01 00 08 63 BB E7 8C 0F AC EB 9A
    [?C??????c???????]
Apr  8 17:45:48.225: RADIUS:   61 69 72 6F 6E 65 74
    [aironet]
Apr  8 17:45:48.225: RADIUS:  Session-Timeout     [27]  6   20
Apr  8 17:45:48.225: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.226: RADIUS(0000001C): Received from id 21645/93
Apr  8 17:45:48.226: RADIUS/DECODE: EAP-Message fragments, 23, total 23 bytes
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp: found eap pak in
```

```
    server response
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp: found session timeout
    20 sec
Apr  8 17:45:48.227: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_REPLY

) for
    0002.8aa6.304f
Apr  8 17:45:48.227: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.227: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:45:48.232: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.232: dot11_auth_dot1x_run_rfsm: Executing Action
    (

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:45:48.233: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.234: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:45:48.234: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.234: RADIUS(0000001C): Using existing nas_port 17
Apr  8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.234: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.234: RADIUS(0000001C): sending
Apr  8 17:45:48.234: RADIUS(0000001C): Send Access-Request to
    10.0.0.3:1645 id 21645/94, len 166
Apr  8 17:45:48.235: RADIUS:  authenticator 93 B5 CC B6 41 97 A0 85
    - 1B 4D 13 0F 6A EE D4 11
Apr  8 17:45:48.235: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.235: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.236: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.236: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.236: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 17:45:48.236: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.236: RADIUS:  EAP-Message         [79]  41
Apr  8 17:45:48.236: RADIUS:   02 43 00 27 11 01 00 18 30 9F 55 AF 05 03 71 7D
    [?C?'????0?U???q}]
Apr  8 17:45:48.236: RADIUS:   25 41 1B B0 F4 A9 7C EE F5 51 24 9A FC 6D 51 6D
    [?A????|??Q$??mQm]
Apr  8 17:45:48.237: RADIUS:   61 69 72 6F 6E 65 74                  [aironet]
Apr  8 17:45:48.237: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless   [19]
Apr  8 17:45:48.237: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.238: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.238: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.242: RADIUS: Received from id 21645/94 10.0.0.3:1645,
    Access-Challenge, len 50
Apr  8 17:45:48.243: RADIUS:  authenticator 59 2D EE 24 CF B2 87 AF
    - 86 D0 C9 00 79 BE 6E 1E
Apr  8 17:45:48.243: RADIUS:  EAP-Message         [79]  6
Apr  8 17:45:48.243: RADIUS:   03 43 00 04
    [?C??]
```

```
Apr  8 17:45:48.244: RADIUS:  Session-Timeout     [27]  6   20
Apr  8 17:45:48.244: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.244: RADIUS(0000001C): Received from id 21645/94
Apr  8 17:45:48.244: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:45:48.244: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Apr  8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp:
    found session timeout 20 sec
Apr  8 17:45:48.245: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_REPLY

)
for 0002.8aa6.304f
Apr  8 17:45:48.245: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.246: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:45:48.249: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.250: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 17:45:48.250: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.250: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:45:48.250: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.251: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:45:48.251: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.251: RADIUS(0000001C): Using existing nas_port 17
Apr  8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.252: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.252: RADIUS(0000001C): sending
Apr  8 17:45:48.252: RADIUS(0000001C): Send Access-Request to
    10.0.0.3:1645 id 21645/95, len 150
Apr  8 17:45:48.252: RADIUS:  authenticator 39 1C A5 EF 86 9E BA D1
    - 50 FD 58 80 A8 8A BC 2A
Apr  8 17:45:48.253: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.253: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.253: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.253: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.254: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 17:45:48.254: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.254: RADIUS:  EAP-Message         [79]  25
Apr  8 17:45:48.254: RADIUS:   01 43 00 17 11 01 00 08 50 9A 67 2E 7D 26 75 AA
    [?C??????P?g.}&u?]
Apr  8 17:45:48.254: RADIUS:   61 69 72 6F 6E 65 74
    [aironet]
Apr  8 17:45:48.254: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless  [19]
Apr  8 17:45:48.254: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.255: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.255: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.260: RADIUS: Received from id 21645/95 10.0.0.3:1645,
```

```
    Access-Accept, len 206
Apr  8 17:45:48.260: RADIUS:  authenticator 39 13 3C ED FC 02 68 63
    - 24 13 1B 46 CF 93 B8 E3
Apr  8 17:45:48.260: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr  8 17:45:48.261: RADIUS:  EAP-Message         [79]  41
Apr  8 17:45:48.261: RADIUS:   02 00 00 27 11 01 00 18 FA 53 D0 29 6C 9D 66 8E
    [???'?????S?)l?f?]
Apr  8 17:45:48.262: RADIUS:   C4 A3 CD 54 08 8C 35 7C 74 0C 6A EF D4 6D 30 A4
    [???T??5|t?j??m0?]
Apr  8 17:45:48.262: RADIUS:   61 69 72 6F 6E 65 74                  [aironet]
Apr  8 17:45:48.262: RADIUS:  Vendor, Cisco       [26]  59
Apr  8 17:45:48.262: RADIUS:   Cisco AVpair       [1]   53
    "leap:session-key=G:3asil;mwerAEJNYH-JxI,"
Apr  8 17:45:48.262: RADIUS:  Vendor, Cisco       [26]  31
Apr  8 17:45:48.262: RADIUS:   Cisco AVpair       [1]   25
    "auth-algo-type=eap-leap"
Apr  8 17:45:48.262: RADIUS:  Class               [25]  31
Apr  8 17:45:48.263: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 64 36
    [CISCOACS:00001d6]
Apr  8 17:45:48.263: RADIUS:   33 2F 30 61 30 30 30 30 36 36 2F 31 37
    [3/0a000066/17]
Apr  8 17:45:48.263: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.264: RADIUS(0000001C): Received from id 21645/95
Apr  8 17:45:48.264: RADIUS/DECODE: EAP-Message fragments, 39, total 39 bytes
Apr  8 17:45:48.264: found leap session key
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: PASS
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    found leap session key in server response
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    leap session key length 16
Apr  8 17:45:48.266: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_PASS

) for 0002.8aa6.304f
Apr  8 17:45:48.266: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.266: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:45:48.266: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station RKIBBE-W2K4 0002.8aa6.304f Associated KEY_MGMT[NONE]
```

注意 state-machine 调试中的状态流。状态流在几种状态之间变化：

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY

注意：当两个协商时，可以有多个CLIENT_WAIT和CLIENT_REPLY的迭代，以及SERVER_WAIT和SERVER_REPLY。

6. SERVER_PASS

process 调试显示每种状态中的每个步骤。radius 调试显示身份验证服务器和客户端之间的实际对话。使用 EAP 调试的最简单方法是注意状态机消息在每种状态之间的变化。

协商中一些内容失败时，state-machine 调试显示过程停止的原因。注意类似于以下示例的消息：

- **CLIENT TIMEOUT** — 此状态表明客户端未在适当的时间段内做出响应。可能由于以下原因而出现无法响应的情况：
  - 客户端软件存在问题。
  - EAP 客户端超时值（在“Advanced Security”下的“EAP Authentication”子选项卡中）已过期。

  一些 EAP（特别是受保护的 EAP (PEAP)）完成身份验证需要超过 30 秒的时间。请将此计时器设置为较高的值（90 和 120 秒之间）。

  下面是 CLIENT TIMEOUT 尝试的示例：

CLIENT TIMEOUT 示例

```
<#root>

Apr 12 17:51:09.373: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Apr 12 17:51:09.373: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0040.96a0.3758
Apr 12 17:51:09.374: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr 12 17:51:39.358: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,TIMEOUT

) for 0040.96a0.3758
Apr 12 17:51:39.358: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0040.96a0.3758
Apr 12 17:51:39.358: %DOT11-7-AUTH_FAILED:
    Station 0040.96a0.3758 Authentication failed
```

  注意：注意与以下消息类似的任何系统错误消息：

```
%DOT11-4-MAXRETRIES: Packet to client xxxx.xxxx.xxxx reached
          max retries, removing the client
```

注意：此类错误消息可能表示存在射频(RF)问题。

- 共享密钥在 AP 和 RADIUS 服务器之间不匹配 — 在以下示例日志中，RADIUS 服务器不接受来自 AP 的身份验证请求。AP 继续向 RADIUS 服务器发送请求，但是 RADIUS 服务器拒绝该请求，因为共享密钥不匹配。

  要解决此问题，请确保检查 AP 上的共享密钥与在 RADIUS 服务器中使用的共享密钥是否相同。

共享密钥在 AP 和 RADIUS 服务器之间不匹配
Jun 2 15:58:13.553: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.10.1.172:1645, 1646 is not responding. Jun 2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.10.1.172:1645,1646 has returned. Jun 2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758 Authentication failed

- **server_timeout** — 此状态表明身份验证服务器未在适当的时间段内做出响应。由于服务器存在问题而出现无法响应的情况。验证是否满足以下情况：
  - AP 具有与身份验证服务器的 IP 连接。

    注意：您可以使用ping命令来验证连接。
  - 服务器的身份验证和计费端口号正确。

    注意：可以从“服务器管理器”(Server Manager)选项卡检查端口号。
  - 身份验证服务正在运行并且可以正常发挥作用。

  下面是 server_timeout 尝试的示例：

server_timeout 示例
<#root> Apr 8 20:02:55.469: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start Apr 8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client: sending identity request for 0002.8aa6.304f Apr 8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client: Started timer client_timeout 30 seconds Apr 8 20:02:55.470: dot11_auth_parse_client_pak: Received EAPOL packet from 0002.8aa6.304f Apr 8 20:02:55.470: dot11_auth_dot1x_run_rfsm: Executing Action(**CLIENT_WAIT,EAP_START**

```
) for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr  8 20:02:55.471: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.472: dot11_auth_parse_client_pak:
    id is not matching req-id:1resp-id:2, waiting for response
Apr  8 20:02:55.474: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 20:02:55.475: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [248] 14
Apr  8 20:02:55.476: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [150] 2
Apr  8 20:02:55.476: RADIUS(00000031): Storing nasport 32 in rad_db
Apr  8 20:02:55.476: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.476: RADIUS/ENCODE(00000031): acct_session_id: 49
Apr  8 20:02:55.477: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.477: RADIUS(00000031): sending
Apr  8 20:02:55.477: RADIUS(00000031): Send Access-Request
    to 10.0.0.3:1234 id 21645/145, len 139
Apr  8 20:02:55.478: RADIUS:  authenticator B6 F7 BB 41 0E 9F 44 D1
    - 9A F8 E2 D7 5D 70 F2 76
Apr  8 20:02:55.478: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 20:02:55.478: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 20:02:55.478: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 20:02:55.478: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 20:02:55.478: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 20:02:55.478: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 20:02:55.478: RADIUS:  EAP-Message         [79]  14
Apr  8 20:02:55.479: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
    [?????aironet]
Apr  8 20:02:55.479: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless [19]
Apr  8 20:02:55.479: RADIUS:  NAS-Port            [5]   6   32
Apr  8 20:02:55.479: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 20:02:55.480: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 20:03:00.478: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:05.475: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:10.473: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS:
    No response from (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS/DECODE:
    parse response no app start; FAIL
Apr  8 20:03:15.470: RADIUS/DECODE:
    parse response; FAIL
```

```
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    detailed aaa_status 1
Apr  8 20:03:15.471: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_FAIL

) for 0002.8aa6.304f
Apr  8 20:03:15.471: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0002.8aa6.304f
Apr  8 20:03:15.471: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
    Authentication failed
```

- **SERVER_FAIL** — 此状态表明服务器基于用户凭据做出了不成功的身份验证响应。此故障前面的 RADIUS 调试显示提供给身份验证服务器的用户名。确保检查身份验证服务器中的“Failed Attempts”日志，以了解有关服务器拒绝客户端访问的其他详细信息。

下面是 SERVER_FAIL 尝试的示例：

SERVER_FAIL 示例

```
<#root>

Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:46:13.605: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:46:13.605: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:46:13.606: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:46:13.606: RADIUS(0000001D): Using existing nas_port 18
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS/ENCODE(0000001D): acct_session_id: 29
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS(0000001D): sending
Apr  8 17:46:13.607: RADIUS(0000001D): Send Access-Request
    to 10.0.0.3:1645 id 21645/97, len 176
Apr  8 17:46:13.607: RADIUS:  authenticator 88 82 8C BB DC 78 67 76
    - 36 88 1D 89 2B DC C9 99
Apr  8 17:46:13.607: RADIUS:  User-Name           [1]   14  "unknown_user"
Apr  8 17:46:13.607: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:46:13.608: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:46:13.608: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:46:13.608: RADIUS:  Service-Type        [6]   6   Login   [1]
Apr  8 17:46:13.608: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.608: RADIUS:  EAP-Message         [79]  46
Apr  8 17:46:13.608: RADIUS:  02 44 00 2C 11 01 00 18 02
    69 C3 F1 B5 90 52 F7    [?D?,?????i????R?]
Apr  8 17:46:13.609: RADIUS:
    B2 57 FF F0 74 8A 80 59 31 6D C7 30 D3 D0 AF 65
```

```
    [?W??t??Y1m?O???e]
Apr  8 17:46:13.609: RADIUS:   75 6E 6B 6E 6F 77 6E 5F 75 73 65 72
    [unknown_user]
Apr  8 17:46:13.609: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless           [19]
Apr  8 17:46:13.609: RADIUS:  NAS-Port            [5]   6   18
Apr  8 17:46:13.610: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:46:13.610: RADIUS:  Nas-Identifier      [32]  16
    "labap1200ip102"
Apr  8 17:46:13.622: RADIUS: Received from id 21645/97
    10.0.0.3:1645,

Access-Reject

, len 56
Apr  8 17:46:13.622: RADIUS:  authenticator 55 E0 51 EF DA CE F7 78
    - 92 72 3D 97 8F C7 97 C3
Apr  8 17:46:13.622: RADIUS:  EAP-Message         [79]  6
Apr  8 17:46:13.623: RADIUS:   04 44 00 04                          [?D??]
Apr  8 17:46:13.623: RADIUS:  Reply-Message       [18]  12
Apr  8 17:46:13.623: RADIUS:   52 65 6A 65 63 74 65 64 0A 0D  [Rejected??]
Apr  8 17:46:13.623: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.624: RADIUS(00000001D): Received from id 21645/97
Apr  8 17:46:13.624: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:46:13.624: RADIUS/DECODE: Reply-Message fragments,
    10, total 10 bytes
Apr  8 17:46:13.624: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: FAIL
Apr  8 17:46:13.625: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:46:13.625: dot11_auth_dot1x_run_rfsm:
    xecuting Action(

SERVER_WAIT,SERVER_FAIL

) for 0002.8aa6.304f
Apr  8 17:46:13.625: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:46:13.626: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:46:13.626: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-6-DISASSOC: Interface Dot11Radio0,
    Deauthenticating Station 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
    Authentication failed
```

- 没有来自客户端的响应 — 在此示例中，RADIUS 服务器向 AP 发送通行消息（AP 继续转发该通行消息），然后它与客户端相关联。最终，客户端未对 AP 做出响应。因此，达到最大尝试次数后 AP 取消对它的身份验证。

没有来自客户端的响应
<#root>

```
Sep 22 08:42:04: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 08:42:04: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station arlit1ad1hd6j91 0040.96a0.3758 Associated KEY_MGMT[NONE]
Sep 22 10:35:10: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached

max retries

, removing the client
Sep 22 10:35:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,


Deauthenticating Station

 0040.96a0.3758
    Reason: Previous authentication no longer valid
```

AP 将获得质询响应从 RADIUS 转发到客户端。客户端未响应并且达到了最大尝试次数，这导致 EAP 失败并且 AP 取消对客户端的身份验证。

没有来自客户端的响应

<#root>

```
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Sep 22 10:43:02: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 10:43:05: %DOT11-4-MAXRETRIES: Packet to client 0040.96a0.3758
    reached

max retries

, removing the client
Sep 22 10:43:05: Client 0040.96a0.3758 failed: reached maximum retries
```

RADIUS 向 AP 发送通行消息，AP 将通行消息转发给客户端，但是客户端未做出响应。达到最大尝试次数后 AP 取消对它的身份验证。客户端然后尝试向 AP 发送新身份请求，但是 AP 拒绝此请求，因为客户端已达到最大尝试次数。

没有来自客户端的响应

```
<#root>

Sep 22 10:57:08: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 10:57:08: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station arlit1ad1hd6j91 0040.96a0.3758 Reassociated KEY_MGMT[NONE]
Sep 22 10:57:10: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached max retries, removing the client
Sep 22 10:57:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,
    Deauthenticating Station0040.96a0.3758 Reason:
    Previous authentication no longer valid
Sep 22 10:57:15: AAA/BIND(00001954): Bind i/f
Sep 22 10:57:15: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
    Sending identity request to 0040.96a0.3758
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
    Client 0040.96a0.3758 timer started for 30 seconds
Sep 22 10:57:15: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached

max retries

, removing the client
Sep 22 10:57:15: Client 0040.96a0.3758 failed: reached maximum retries
```

紧接在状态机消息前面的**process** 和/或**radius** 调试显示故障的详细信息。

有关如何配置 EAP 的详细信息，请参阅使用 RADIUS 服务器执行 EAP 身份验证。

MAC 验证

以下调试对于 MAC 身份验证非常有帮助：

- debug radius authentication — 使用外部身份验证服务器时，此调试的输出以下面的词开头：RADIUS.
- debug dot11 aaa authenticator mac-authen — 此调试的输出以下面的文本开头：dot11_auth_dot1x_。

这些调试显示：

- 在身份验证对话框的 RADIUS 部分期间报告的内容
- 给定的 MAC 地址与身份验证所依据的 MAC 地址之间的比较

使用外部 RADIUS 服务器进行 MAC 地址身份验证时，RADIUS 调试适用。此连接的结果显示身份验证服务器与客户端之间的实际对话。

MAC 地址列表作为用户名和密码数据库在本地构建到设备时，仅 mac-authen 调试显示输出。确定地址是否匹配时，将显示这些输出。

注意：始终在MAC地址中输入任何字母字符（小写）。

以下示例显示依据本地数据库进行的成功的 MAC 身份验证：

成功的 MAC 身份验证示例

```
Apr  8 19:02:00.109: dot11_auth_mac_start: method_list: mac_methods
Apr  8 19:02:00.109: dot11_auth_mac_start: method_index: 0x4500000B, req: 0xA7626C
Apr  8 19:02:00.109: dot11_auth_mac_start: client->unique_id: 0x28
Apr  8 19:02:00.110: dot11_mac_process_reply: AAA reply for 0002.8aa6.304f PASSED
Apr  8 19:02:00.145: %DOT11-6-ASSOC: Interface Dot11Radio0, Station RKIBBE-W2K4
    0002.8aa6.304f Associated KEY_MGMT[NONE]
```

以下示例显示依据本地数据库进行的失败的 MAC 身份验证：

失败的 MAC 身份验证示例

```
Apr  8 19:01:22.336: dot11_auth_mac_start: method_list: mac_methods
Apr  8 19:01:22.336: dot11_auth_mac_start: method_index: 0x4500000B,
    req: 0xA7626C
Apr  8 19:01:22.336: dot11_auth_mac_start: client->unique_id: 0x27
Apr  8 19:01:22.337: dot11_mac_process_reply:
    AAA reply for 0002.8aa6.304f FAILED
Apr  8 19:01:22.337: %DOT11-7-AUTH_FAILED:
    Station 0002.8aa6.304f Authentication failed
```

MAC 地址身份验证失败时，请检查在 MAC 地址中输入的字符的准确性。确保以小写输入 MAC 地址中的所有字母字符。

有关如何配置 MAC 身份验证的详细信息，请参阅配置身份验证类型（用于 Cisco Aironet 接入点的 Cisco IOS 软件 12.2(13)JA 配置指南）。

WPA

尽管 Wi-Fi Protected Access (WPA) 不是身份验证类型，但它是协商协议。

- WPA 在 AP 和客户端卡之间进行协商。
- WPA 密钥管理在身份验证服务器成功验证客户端之后进行协商。
- WPA 在四次握手中协商成对临时密钥 (PTK) 和成组临时密钥 (GTK)。

注意：由于WPA要求基础EAP成功，请在使用WPA之前验证客户端能否成功使用该EAP进行身份验

证。

以下调试对于 WPA 协商非常有帮助：

- debug dot11 aaa authenticator process — 此调试的输出以下面的文本开头：`dot11_auth_dot1x_`。
- debug dot11 aaa authenticator state-machine — 此调试的输出以下面的文本开头：`dot11_auth_dot1x_run_rfsm`。

相对于本文档中的其他身份验证，WPA 调试的阅读和分析非常简单。应该发送 PTK 消息并且收到适当的回复。接下来，应该发送 GTK 消息并且收到另一适当的响应。

如果不发送 PTK 或 GTK 消息，则 AP 上的配置或软件级别可能会出现问题。如果未收到来自客户端的 PTK 或 GTK 响应，请检查客户端卡的 WPA 请求方上的配置或软件级别。

成功的 WPA 协商示例

```
<#root>

labap1200ip102#

Apr  7 16:29:57.908: dot11_dot1x_build_ptk_handshake:
    building PTK msg 1 for 0030.6527.f74a

Apr  7 16:29:59.190: dot11_dot1x_verify_ptk_handshake:
    verifying PTK msg 2 from 0030.6527.f74a

Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key len (exp=0x20, act=0x0)

Apr  7 16:29:59.192: dot11_dot1x_build_ptk_handshake:
    building PTK msg 3 for 0030.6527.f74a

Apr  7 16:29:59.783: dot11_dot1x_verify_ptk_handshake:
    verifying PTK msg 4 from 0030.6527.f74a

Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key len (exp=0x20, act=0x0)

Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
    building GTK msg 1 for 0030.6527.f74a

Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
    dot11_dot1x_get_multicast_key len 32 index 1
Apr  7 16:29:59.788: dot11_dot1x_hex_dump: GTK:
    27 CA 88 7D 03 D9 C4 61 FD 4B BE 71 EC F7 43 B5 82 93 57 83

Apr  7 16:30:01.633: dot11_dot1x_verify_gtk_handshake:
    verifying GTK msg 2 from 0030.6527.f74a

Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header:
    Warning: Invalid key info (exp=0x391, act=0x301
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key len (exp=0x20, act=0x0)
```

```
Apr  7 16:30:01.633: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station   0030.6527.f74a Associated KEY_MGMT[WPA]

labap1200ip102#
```

有关如何配置 WPA 的详细信息，请参阅 WPA 配置概述。

管理/HTTP 身份验证

可以限制只有在本地用户名和密码数据库中列出的用户或者外部身份验证服务器可以对设备进行管理访问。RADIUS 和 TACACS+ 都支持管理访问。

以下调试对于管理身份验证非常有帮助：

- debug radius authentication 或 debug tacacs authentication — 此调试的输出以下面的词之一开头：RADIUS 或 TACACS。
- debug aaa authentication — 此调试的输出以下面的文本开头：AAA/AUTHEN。
- debug aaa authorization — 此调试的输出以下面的文本开头：AAA/AUTHOR。

这些调试显示：

- 在身份验证对话框的 RADIUS 或 TACACS 部分期间报告的内容
- 设备与身份验证服务器之间的实际身份验证和授权协商

以下示例显示 Service-Type RADIUS 属性设置为 Administrative 时的成功管理身份验证：

具有 Service-Type 属性的成功管理身份验证示例

```
<#root>

Apr 13 19:43:08.030: AAA: parse name=tty2 idb type=-1 tty=-1
Apr 13 19:43:08.030: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0
    adapter=0 port=2 channel=0
Apr 13 19:43:08.031: AAA/MEMORY: create_user (0xA1BB6C) user='NULL' ruser='NULL'
    ds0=0 port='tty2' rem_addr='10.0.0.25' authen_type=ASCII service=LOGINN
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540): port='tty2'
    list='' action=LOGIN service=LOGIN
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540): using "default" list
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540):
    Method=tac_admin (tacacs+)
Apr 13 19:43:08.032: TAC+: send AUTHEN/START packet ver=192 id=3200017540
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=ERROR
Apr 13 19:43:08.032: AAA/AUTHEN/START (3200017540):
    Method=rad_admin (radius)
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETUSER
Apr 13 19:43:08.032: AAA/AUTHEN/CONT (3200017540):
    continue_login (user='(undef)')
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETUSER
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Method=rad_admin (radius)
```

```
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETPASS
Apr 13 19:43:08.033: AAA/AUTHEN/CONT (3200017540):
    continue_login (user='aironet')
Apr 13 19:43:08.033: AAA/AUTHEN(3200017540): Status=GETPASS
Apr 13 19:43:08.033: AAA/AUTHEN(3200017540): Method=rad_admin (radius)
Apr 13 19:43:08.033: RADIUS: Pick NAS IP for u=0xA1BB6C tableid=0
    cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 19:43:08.033: RADIUS: ustruct sharecount=1
Apr 13 19:43:08.034: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 19:43:08.034: RADIUS(00000000): Send Access-Request to 10.0.0.3:1645
    id 21646/48, len 76
Apr 13 19:43:08.034: RADIUS:  authenticator 91 A0 98 87 C1 FC F2 E7
    - E7 E4 57 DF 20 D0 82 27
Apr 13 19:43:08.034: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 19:43:08.034: RADIUS:  NAS-Port            [5]   6   2
Apr 13 19:43:08.035: RADIUS:  NAS-Port-Type       [61]  6   Virtual         [5]
Apr 13 19:43:08.035: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 19:43:08.035: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 19:43:08.035: RADIUS:  User-Password       [2]   18  *
Apr 13 19:43:08.042: RADIUS: Received from id 21646/48 10.0.0.3:1645,
    Access-Accept, len 62
Apr 13 19:43:08.042: RADIUS:  authenticator C9 32 E7 8F 97 5F E6 4C
    - 6B 90 71 EE ED 2C 2B 2B
Apr 13 19:43:08.042:

RADIUS:  Service-Type        [6]   6
    Administrative            [6]

Apr 13 19:43:08.042: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 19:43:08.042: RADIUS:  Class               [25]  30
Apr 13 19:43:08.043: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 36
    [CISCOACS:0000366]
Apr 13 19:43:08.043: RADIUS:   39 2F 30 61 30 30 30 30 36 36 2F 32
    [9/0a000066/2]
Apr 13 19:43:08.044: RADIUS: saved authorization data for user A1BB6C at B0C260
Apr 13 19:43:08.044: AAA/AUTHEN(3200017540): Status=PASS
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147):
    Port='tty2' list='' service=EXEC
Apr 13 19:43:08.044: AAA/AUTHOR/HTTP: tty2(1763745147) user='aironet'
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV service=shell
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV cmd*
Apr 13 19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): found list "default"
Apr 13 19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): Method=tac_admin (tacacs+)
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): user=aironet
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): send AV service=shell
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): send AV cmd*
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147): Post authorization status = ERROR
Apr 13 19:43:08.046: tty2 AAA/AUTHOR/HTTP(1763745147):
    Method=rad_admin (radius)
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147):
    Post authorization status = PASS_ADD
Apr 13 19:43:08.443: AAA/MEMORY: free_user (0xA1BB6C) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII service=LOGIN
```

以下示例显示使用特定于供应商的属性发送“priv-level”语句时的成功管理身份验证：

具有特定于供应商的属性的成功管理身份验证示例

```
<#root>

Apr 13 19:38:04.699: RADIUS: cisco AVPair ""shell:priv-lvl=15""
    not applied for shell
Apr 13 19:38:04.699: AAA/AUTHOR (380584213): Post authorization status
    = PASS_ADD
Apr 13 19:38:04.802: AAA/MEMORY: free_user (0xAA0E38) user='aironet'
    ruser='NULL' port='tty3' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN
Apr 13 19:38:04.901: AAA: parse name=tty3 idb type=-1 tty=-1
Apr 13 19:38:04.901: AAA: name=tty3 flags=0x11 type=5 shelf=0 slot=0
    adapter=0  port=3 channel=0
Apr 13 19:38:04.902: AAA/MEMORY: create_user (0xAA23BC) user='NULL'
    ruser='NULL' ds0=0 port='tty3' rem_addr='10.0.0.25'
    authen_type=ASCII service=LOGIN
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): port='tty3' list=''
    action=LOGIN service=LOGIN
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): using "default" list
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): Method=tac_admin (tacacs+)
Apr 13 19:38:04.902: TAC+: send AUTHEN/START packet ver=192 id=1346300140
Apr 13 19:38:04.902: AAA/AUTHEN(1346300140): Status=ERROR
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.902: AAA/AUTHEN(1346300140): Status=GETUSER
Apr 13 19:38:04.903: AAA/AUTHEN/CONT (1346300140): continue_login
    (user='(undef)')
Apr 13 19:38:04.903: AAA/AUTHEN(1346300140): Status=GETUSER
Apr 13 19:38:04.903: AAA/AUTHEN(1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS
Apr 13 19:38:04.904: AAA/AUTHEN/CONT (1346300140): continue_login
    (user='aironet')
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.904: RADIUS: Pick NAS IP for u=0xAA23BC tableid=0
    cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 19:38:04.904: RADIUS: ustruct sharecount=1
Apr 13 19:38:04.904: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 19:38:04.925: RADIUS(00000000): Send Access-Request to
    10.0.0.3:1645 id 21646/3, len 76
Apr 13 19:38:04.926: RADIUS:  authenticator 0C DD 2B B7 CA 5E 7C B9
    - 46 90 FD 7A FD 56 3F 07
Apr 13 19:38:04.926: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 19:38:04.926: RADIUS:  NAS-Port            [5]   6   3
Apr 13 19:38:04.926: RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
Apr 13 19:38:04.926: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 19:38:04.926: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 19:38:04.926: RADIUS:  User-Password       [2]   18  *
Apr 13 19:38:04.932: RADIUS: Received from id 21646/3 10.0.0.3:1645,
    Access-Accept, len 89
Apr 13 19:38:04.933: RADIUS:  authenticator FA A4 31 49 51 87 9D CA
    - 9D F7 B3 9B EF C2 8B 7E
Apr 13 19:38:04.933: RADIUS:  Vendor, Cisco       [26]  27
Apr 13 19:38:04.933: RADIUS:

   Cisco AVpair     [1]   21  ""shell:priv-lvl=15""

Apr 13 19:38:04.934: RADIUS:  Service-Type        [6]   6   Login       [1]
Apr 13 19:38:04.934: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 19:38:04.934: RADIUS:  Class               [25]  30
Apr 13 19:38:04.934: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 33
    [CISCOACS:0000363]
Apr 13 19:38:04.934: RADIUS:   61 2F 30 61 30 30 30 30 36 36 2F 33
    [a/0a000066/3]
Apr 13 19:38:05.634: AAA/AUTHOR (3854191802): Post authorization
```

```
    status = PASS_ADD
Apr 13 19:38:05.917: AAA/MEMORY: free_user (0xA9D054) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0
```

管理身份验证的最常见问题是无法将身份验证服务器配置为发送适当的权限级别或管理服务类型属性。以下示例尝试的管理身份验证失败，因为未发送权限级别属性或者管理服务类型属性：

无特定于供应商的属性或者服务类型属性

```
<#root>

Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): Port='tty3'
    list=''

service=EXEC

Apr 13 20:02:59.516: AAA/AUTHOR/HTTP: tty3(2007927065) user='aironet'
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): send AV service=shell
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): send AV cmd*
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): found list "default"
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): Method=tac_admin (tacacs+)
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): user=aironet
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send AV service=shell
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send AV cmd*
Apr 13 20:02:59.516: AAA/AUTHOR (2007927065): Post authorization status = ERROR
Apr 13 20:02:59.517: tty3 AAA/AUTHOR/HTTP(2007927065): Method=rad_admin (radius)
Apr 13 20:02:59.517: AAA/AUTHOR (2007927065): Post authorization status = PASS_ADD
Apr 13 20:02:59.561: AAA/MEMORY: free_user (0xA756E8) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0  vrf= (id=0)
Apr 13 20:02:59.620: AAA/MEMORY: free_user (0x9E5B04) user='aironet'
    ruser='NULL'  port='tty3' rem_addr='10.0.0.25' authen_type=ASCII


service=LOGIN

 priv=0 vrf= (id=0)
Apr 13 20:03:04.501: AAA: parse name=tty2 idb type=-1 tty=-1
Apr 13 20:03:04.501: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0
    port=2 channel=0
Apr 13 20:03:04.502: AAA/MEMORY: create_user (0xA9C7A4) user='NULL'
    ruser='NULL' ds0=0 port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): port='tty2' list=''
    action=LOGIN service=LOGIN
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): using "default" list
Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642): Method=tac_admin (tacacs+)
Apr 13 20:03:04.503: TAC+: send AUTHEN/START packet ver=192 id=377202642
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=ERROR
Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642): Method=rad_admin (radius)
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETUSER
Apr 13 20:03:04.503: AAA/AUTHEN/CONT (377202642): continue_login (user='(undef)')
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETUSER
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Method=rad_admin (radius)
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETPASS
Apr 13 20:03:04.504: AAA/AUTHEN/CONT (377202642): continue_login (user='aironet')
Apr 13 20:03:04.504: AAA/AUTHEN(377202642): Status=GETPASS
```

```
Apr 13 20:03:04.504: AAA/AUTHEN(377202642): Method=rad_admin (radius)
Apr 13 20:03:04.504: RADIUS: Pick NAS IP for u=0xA9C7A4 tableid=0
    cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 20:03:04.505: RADIUS: ustruct sharecount=1
Apr 13 20:03:04.505: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 20:03:04.505: RADIUS(00000000): Send Access-Request to 10.0.0.3:1645
    id 21646/59, len 76
Apr 13 20:03:04.505: RADIUS:  authenticator 0F BD 81 17 8F C5 1C B4
    - 84 1C 66 4D CF D4 96 03
Apr 13 20:03:04.505: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 20:03:04.506: RADIUS:  NAS-Port            [5]   6   2
Apr 13 20:03:04.506: RADIUS:  NAS-Port-Type       [61]  6   Virtual           [5]
Apr 13 20:03:04.506: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 20:03:04.506: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 20:03:04.507: RADIUS:  User-Password       [2]   18  *
Apr 13 20:03:04.513: RADIUS: Received from id 21646/59 10.0.0.3:1645,


Access-Accept

, len 56
Apr 13 20:03:04.513: RADIUS:  authenticator BB F0 18 78 33 D0 DE D3
    - 8B E9 E0 EE 2A 33 92 B5
Apr 13 20:03:04.513: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 20:03:04.513: RADIUS:  Class               [25]  30
Apr 13 20:03:04.514: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 38
    [CISCOACS:0000368]
Apr 13 20:03:04.514: RADIUS:   33 2F 30 61 30 30 30 30 36 36 2F 32
    [3/0a000066/2]
Apr 13 20:03:04.515: RADIUS: saved authorization data for user A9C7A4 at A9C99C
Apr 13 20:03:04.515: AAA/AUTHEN(377202642): Status=PASS
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): Port='tty2' list=''
    service=EXEC
Apr 13 20:03:04.515: AAA/AUTHOR/HTTP: tty2(2202245138) user='aironet'
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): send AV service=shell
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): send AV cmd*
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): found list "default"
Apr 13 20:03:04.516: tty2 AAA/AUTHOR/HTTP(2202245138): Method=tac_admin (tacacs+)
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): user=aironet
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send AV service=shell
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send AV cmd*
Apr 13 20:03:04.517:

AAA/AUTHOR

(2202245138):

Post authorization status = ERROR

Apr 13 20:03:04.517: tty2 AAA/AUTHOR/HTTP(2202245138): Method=rad_admin (radius)
Apr 13 20:03:04.517: AAA/AUTHOR (2202245138): Post authorization status
    = PASS_ADD
Apr 13 20:03:04.619: AAA/MEMORY: free_user (0xA9C7A4) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0 vrf=
```

有关如何配置管理身份验证的详细信息，请参阅管理接入点（用于 Cisco Aironet 接入点的 Cisco IOS 软件 12.2(13)JA 配置指南）。

有关如何将管理权限配置为身份验证服务器上的用户的详细信息，请参阅示例配置：HTTP 服务器

用户的本地身份验证。查看与您使用的身份验证协议相符的部分。

相关信息

- 用于 Cisco Aironet 接入点的 Cisco IOS 软件 12.2(13)JA 配置指南
- 使用 RADIUS 服务器进行 EAP 身份验证
- 使用本地 RADIUS 服务器执行 LEAP 身份验证
- 在Cisco Aironet无线安全常见问题
- 无线域服务AP作为AAA服务器配置示例
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。