使用 RADIUS 服务器进行 EAP 身份验证

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络 EAP 或采用 EAP 的开放式身份验证](#)
[定义身份验证服务器](#)
[定义客户端身份验证方法](#)
[验证](#)
[故障排除](#)
[故障排除步骤](#)
[故障排除命令](#)
[相关信息](#)

简介

本文档提供了配置基于 Cisco IOS® 的接入点的示例，以便根据 RADIUS 服务器访问的数据库对无线用户进行可扩展身份验证协议 (EAP) 身份验证。

由于接入点在 EAP 中发挥的被动作用（将无线数据包从客户端桥接到要发送到身份验证服务器的有线数据包，或反向操作），此配置实际上可用于所有 EAP 方法。此类方法包括（但不限于）LEAP、受保护的 EAP (PEAP)-MS-质询握手身份验证协议 (CHAP) 版本 2、PEAP-通用令牌卡 (GTC)、EAP-基于安全隧道的灵活身份验证 (FAST)、EAP-传输层安全 (TLS) 和 EAP-隧道 TLS (TTLS)。 必须针对每种 EAP 方法适当配置身份验证服务器。

本文档涵盖了如何配置接入点 (AP) 和 RADIUS 服务器，本文档的配置示例中的 RADIUS 服务器为 Cisco Secure ACS。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 熟悉 Cisco IOS GUI 或 CLI。
- 熟悉有关 EAP 身份验证的概念。

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 Cisco IOS 的 Cisco Aironet AP 产品。
- 假设在网络中仅有一个虚拟 LAN (VLAN)。
- 成功集成到用户数据库的 RADIUS 身份验证服务器产品。
    - 以下为 Cisco LEAP 和 EAP-FAST 支持的身份验证服务器：
        - Cisco 安全访问控制服务器 (ACS)
        - Cisco Access Registrar (CAR)
        - Funk Steel Belted RADIUS
        - Interlink Merit
    - 以下为 Microsoft PEAP-MS-CHAP 版本 2 和 PEAP-GTC 支持的身份验证服务器：
        - Microsoft Internet 身份验证服务 (IAS)
        - Cisco Secure ACS
        - Funk Steel Belted RADIUS
        - Interlink Merit
        - Microsoft 可授权的其他任何身份验证服务器。

      注意：GTC或一次性密码需要额外的服务，这些服务需要在客户端和服务器端使用额外的软件，以及硬件或软件令牌生成器。
    - 请咨询客户端制造商，了解在使用 EAP-TLS、EAP-TTLS 和其他 EAP 方法时，其产品所支持的身份验证服务器。

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。

配置

此配置介绍了如何在基于 IOS 的 AP 上配置 EAP 身份验证。本文档中的示例将 LEAP 作为与 RADIUS 服务器一起使用的 EAP 身份验证方法。

注意：要获取此部分中所用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

与大多数基于口令的身份验证算法一样，Cisco LEAP 很容易受到字典攻击。这并不涉及新型攻击或意味着 Cisco LEAP 的新漏洞。创建强口令策略是降低字典攻击威胁的最有效方式。该方式包括使用强口令以及口令定期失效。有关字典攻击以及如何阻止此类攻击的详细信息，请参阅对 Cisco LEAP 的字典攻击。

本文档中的 GUI 和 CLI 均使用以下配置：

- AP 的 IP 地址为 10.0.0.106。
- RADIUS 服务器 (ACS) 的 IP 地址为 10.0.0.3。

网络 EAP 或采用 EAP 的开放式身份验证

在任何基于 EAP/802.1x 的身份验证方法中，您可能会对网络 EAP 和采用 EAP 的开放式身份验证之间的区别存在疑问。以上两者涉及管理和关联数据包报头中的“身份验证算法”字段中的值。大多数无线客户端制造商将此字段的值设置为 0（开放式身份验证），然后发信号希望在稍后的关联进程中进行 EAP 身份验证。Cisco 对该值的设置有所不同（从与网络 EAP 标志的关联开始时）。

如果网络包含以下客户端：

- Cisco 客户端 - 使用网络 EAP。
- 第三方客户端（包括与 CCX 兼容的产品）- 使用采用 EAP 的开放式身份验证。
- Cisco 客户端与第三方客户端的组合 - 同时选择网络 EAP 和采用 EAP 的开放式身份验证。

定义身份验证服务器

EAP 配置的第一步是定义身份验证服务器，并建立与该服务器的关系。

1. 在接入点的 Server Manager 选项卡（Security > Server Manager 菜单项下）上完成以下步骤：

    a. 在 Server 字段中输入身份验证服务器的 IP 地址。

    b. 指定 Shared Secret 和端口。

    c. 单击 Apply，以创建定义并填充下拉列表。

    d. 在 Default Server Priorities 下，将 EAP Authentication 类型的 Priority 1 字段设置为该服务器 IP 地址。

    e. 单击 Apply。

    也可从 CLI 中发出以下命令：

    <#root>

```
AP#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#
aaa group server radius rad_eap

AP(config-sg-radius)#
server 10.0.0.3 auth-port 1645 acct-port 1646

AP(config-sg-radius)#
exit

AP(config)#
aaa new-model

AP(config)#
aaa authentication login eap_methods group rad_eap

AP(config)#
radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102

AP(config)#
end

AP#
write memory
```

2. 必须在身份验证服务器中将接入点配置为 AAA 客户端。

   例如，在 Cisco Secure ACS 中，可在 Network Configuration 页中完成此操作，该页中可定义接入点名称、IP 地址、共享密钥和身份验证方法（RADIUS Cisco Aironet 或 RADIUS Cisco IOS/PIX）。有关其他非 ACS 身份验证服务器的信息，请参阅制造商提供的文档。

   请确保已相应配置身份验证服务器，以执行所需的 EAP 身份验证方法。例如，对于要执行 LEAP 的 Cisco Secure ACS，请在 System Configuration - Global Authentication Setup 页上配置 LEAP 身份验证。单击 System Configuration，然后单击 Global Authentication Setup。有关其他非 ACS 身份验证服务器或其他 EAP 方法的信息，请参阅制造商提供的文档。

   此图像显示了针对 PEAP、EAP-FAST、EAP-TLS、LEAP 和 EAP-MD5 进行了相应配置的 Cisco Secure ACS。

定义客户端身份验证方法

当接入点知道发送客户端身份验证请求的目标地址之后，请将接入点配置为接受此类身份验证方法。

注意：这些说明适用于基于WEP的安装。有关 WPA（使用的是 Cipher 而不是 WEP）的信息，请参阅 WPA 配置概述。

1. 在接入点的 Encryption Manager 选项卡（Security > Encryption Manager 菜单项下）上完成以下步骤：

    a. 指定要使用 WEP Encryption。

    b. 指定 WEP 为 Mandatory。

    c. 确认是否已将密钥大小设置为 128 位。

    d. 单击 Apply。

    也可从 CLI 中发出以下命令：

```
<#root>
AP#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#
interface dot11radio 0

AP(config-if)#
encryption mode wep mandatory

AP(config-if)#
end

AP#
write memory
```

2. 在接入点的 SSID Manager 选项卡（Security > SSID Manager 菜单项下）上完成以下步骤：

    a. 选择所需的 SSID。

    b. 在“Authentication Methods Accepted”下，选中标记为 Open 的复选框，并使用下拉列表

选择 With EAP。

c. 如果拥有 Cisco 客户端卡，请选中标记为 Network-EAP 的复选框。请参阅网络 EAP 或采用 EAP 的开放式身份验证部分中的讨论。

d. 单击 Apply。

也可从 CLI 中发出以下命令：

```
<#root>

AP#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#
interface dot11radio 0

AP(config-if)#
ssid labap1200

AP(config-if-ssid)#
authentication open eap eap_methods

AP(config-if-ssid)#
authentication network-eap eap_methods

AP(config-if-ssid)#
end

AP#
write memory
```

确认了基本 EAP 配置的基本功能之后，可在随后添加其他功能和密钥管理。在基础功能之上分层添加更多复杂功能，可以简化故障排除步骤。

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令，使用此工具可以查看对 show 命令输出的分析。

- show radius server-group all - 显示 AP 上所有已配置的 RADIUS 服务器组的列表。

故障排除

故障排除步骤

完成以下步骤，对配置进行故障排除。

1. 在客户端实用程序或软件中，使用相同或相似参数创建新的配置文件或连接，以确保在客户端的配置中未发生损坏。
2. 为了排除会阻止成功进行身份验证的 RF 问题，请采取以下所示步骤临时禁用身份验证：
   - 在 CLI 中，使用 no authentication open eap eap_methods、no authentication network-eap eap_methods 和 authentication open 命令。
   - 在 GUI 中，在 SSID Manager 页上取消选中 Network-EAP、选中 Open 并将下拉列表设置回 No Addition。

   如果客户端成功关联，则 RF 与关联问题无关。
3. 确认共享密钥口令已在接入点和身份验证服务器之间同步。否则，可能会收到以下错误消息：

   ```
   Invalid message authenticator in EAP request
   ```

   - 在 CLI 中，检查 `radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>` 行。
   - 在 GUI 中，在 Server Manager 页上标记为“Shared Secret”的框中重新输入相应服务器的共享密钥。

   RADIUS 服务器上接入点的共享密钥条目必须包含与上述相同的共享密钥口令。
4. 从 RADIUS 服务器删除所有用户组。有时，RADIUS 服务器定义的用户组和基础域中的用户组之间会发生冲突。检查 RADIUS 服务器日志中记录的失败尝试和尝试失败的原因。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 show 命令，使用此工具可以查看对 show 命令输出的分析。

调试身份验证中提供了有关如何收集和解释关于 EAP 的 debug 命令输出的大量详细信息。

注意：在发出debug命令之前，请参阅有关Debug命令的重要信息。

- debug dot11 aaa authenticator state-machine — 显示客户端和身份验证服务器之间协商的主

要分区（或状态）。以下为成功进行身份验证时的输出：

<#root>

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
        identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
        0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
        Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:


Sending identity request to 0040.96ac.dd05 (client)

*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
        0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
        Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:


Sending client 0040.96ac.dd05 data (User Name) to server

*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
        Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
        Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:


Forwarding server message(Challenge) to client 0040.96ac.dd05

*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
        Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
        Action(CLIENT_WAIT,CL IENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:


Sending client 0040.96ac.dd05 data(User Credentials) to server

-------------------Lines Omitted for simplicity-------------------
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
        Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
        (SERVER_WAIT,

SE RVER_PASS)

 for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:


Forwarding server message(Pass Message) to client
        0040.96ac.dd05

*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
        Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC:

 Interface Dot11Radio0,
        Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
```

```
        associated to the access point)
```

注意：在12.2(15)JA之前的Cisco IOS软件版本中，此debug命令的语法为debug dot11 aaa dot1x state-machine。

- debug dot11 aaa authenticator process — 显示客户端和身份验证服务器之间协商的单个对话条目。

  注意：在12.2(15)JA之前的Cisco IOS软件版本中，此debug命令的语法为debug dot11 aaa dot1x process。

- debug radius authentication - 显示服务器和客户端（均由 AP 桥接）之间的 RADIUS 协商。以下为身份验证失败时的输出：

<#root>

```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config
```

NAS IP: 10.0.0.106

```
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
*Mar 1 02:34:55.087: RADIUS(00000031):
```

Send Access-Request
**   to 10.0.0.3 :164 5 id 1645/61, len 130**

```
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
        56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS:
```

User-Name [1] 8 "wirels"

```
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS:
```

Calling-Station-Id [31] 16 "0040.96ac.dd05"

```
*Mar 1 02:34:55.088: RADIUS:
```

Service-Type [6] 6 Login [1

```
]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
        4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS:
```

```
Received from id 1645/61
        10.0.0.3 :1645, Access-Challenge, len 79

*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
        84 87 49 9B B4 77 B8 973
--------------------------Lines Omitted-----------------------------------
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031):

Send Access-Request to
        10.0.0.3 :164 5 id 1645/62, len 168


*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
        07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
---------------------------------Lines Omitted----------------------
*Mar 1 02:34:55.124: RADIUS:

Received from id 1645/62
        10.0.0.3 :1645, Access-Reject, len 56

*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
        AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS:

 Reply-Message [18] 12

*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D


[Rejected??]

*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED:

Station
        0040.96ac.dd05 Authentication failed
```

- debug aaa authentication - 显示客户端设备和身份验证服务器之间针对身份验证的 AAA 协商。

相关信息

- 调试身份验证
- 配置身份验证类型
- 本地 RADIUS 服务器上的 LEAP 身份验证
- 配置 RADIUS 和 TACACS+ 服务器
- 对 Cisco Secure ACS for Windows v3.2 配置 PEAP-MS-CHAPv2 机器身份验证

- 对 Cisco Secure ACS for Windows v3.2 配置 EAP-TLS 机器身份验证
- 在 Microsoft IAS 上配置 PEAP/EAP
- 对作为 RADIUS 服务器的 Microsoft IAS 进行故障排除
- Microsoft 802.1X 身份验证客户端
- 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）。