本地 RADIUS 服务器上的 LEAP 身份验证

目录

简介

本文为轻量级扩展身份认证协议(LEAP)验证提供一配置示例在IOS基于®的接入点，为无线客户端服务，以及作为一个本地RADIUS服务器。此配置适用于运行 12.2(11)JA 或更高版本的 IOS 接入点。

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 IOS GUI 或 CLI
- 熟悉与 LEAP 身份验证有关的概念

组件

本文档中的信息基于以下软件和硬件版本。

- Cisco Aironet 1240AG 系列接入点
- Cisco IOS 软件版本 12.3(8)JA2
- 运行 Aironet Desktop Utility 3.6.0.122 的 Cisco Aironet 802.11 a/b/g 无线适配器
- 假设网络中仅有一个 VLAN

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。

本地 RADIUS 服务器功能概述

通常将使用一个外部 RADIUS 服务器度用户进行身份验证。在某些情况下，这不是一个可行的解决方案。此时，可让一个接入点充当 RADIUS 服务器。将按照在接入点中配置的本地数据库来对用户进行身份验证。此功能称为本地 RADIUS 服务器功能。您也可让网络中的其他接入点使用某个接入点上的本地 RADIUS 服务器功能。有关这方面的详细信息，请参阅配置其他接入点以使用本地身份验证器。

配置

该配置描述了如何在某个接入点上配置 LEAP 和本地 Radius 服务器功能。本地 RADIUS 服务器功能是在 Cisco IOS 软件版本 12.2(11)JA 中推出的。有关如何通过外部 RADIUS 服务器来配置 LEAP 的背景信息，请参阅 RADIUS 服务器的 LEAP 身份验证。

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。为了缓解字典攻击，您必须创建强口令策略，其中包括强口令和频繁使用的新口令。有关字典攻击和如何阻止此类攻击的详细信息，请参阅对 Cisco LEAP 的字典攻击。

本文档假设 CLI 和 GUI 均使用以下配置：

1. 接入点的 IP 地址为 **10.77.244.194**。
2. 所用的 SSID 是 **cisco**，它将映射到 **VLAN 1**。
3. 用户名是 **user1** 和 **user2**，它们将映射到组 **Testuser**。

CLI 配置

接入点

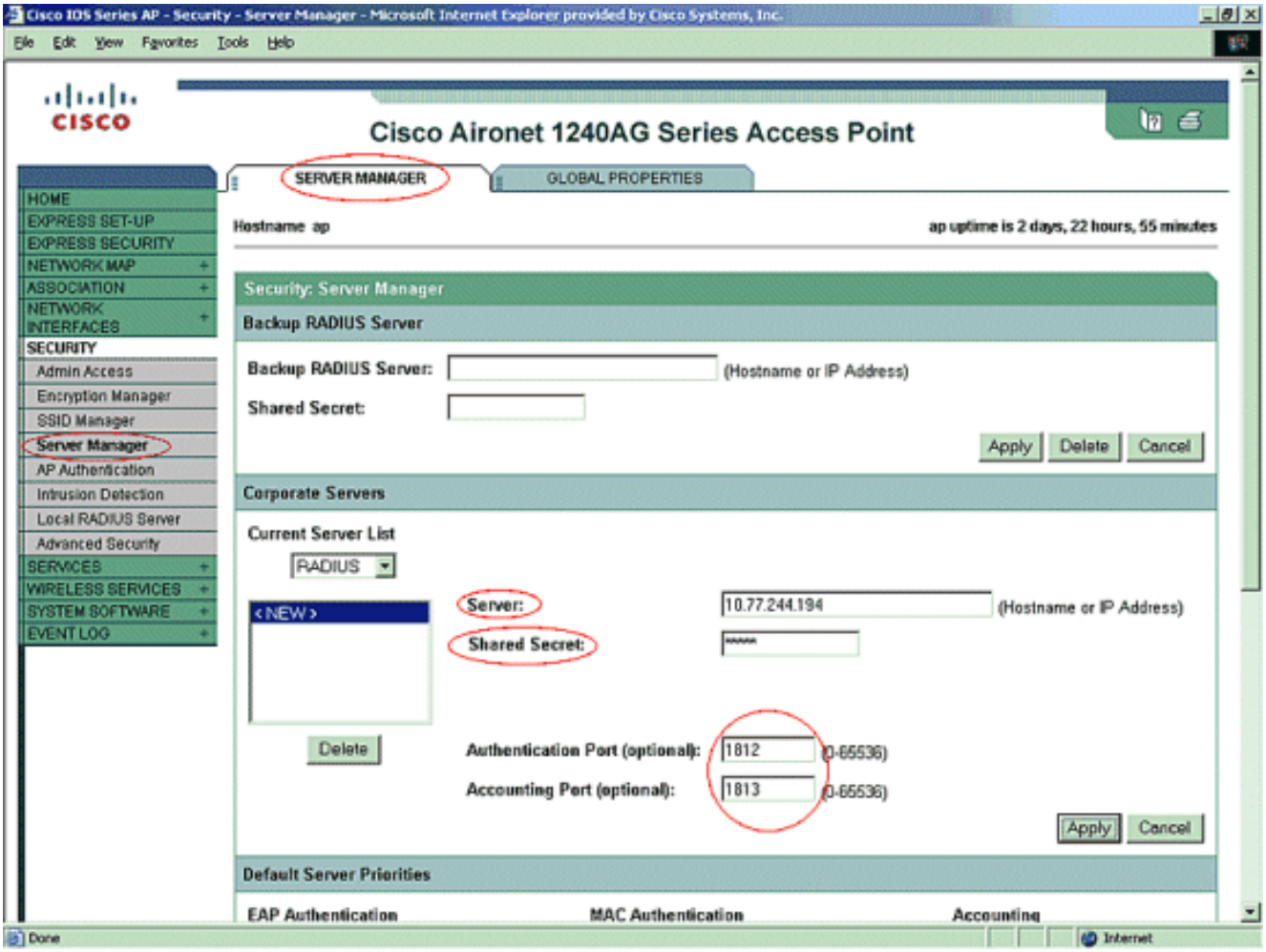
```
ap#show running-config Building configuration... . . .
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap server
10.77.244.194 auth-port 1812 acct-port 1813 !--- A
server group for RADIUS is created called "rad_eap" !---
that uses the server at 10.77.244.194 on ports 1812 and
1813. . . . aaa authentication login eap_methods group
rad_eap !--- Authentication [user validation] is to be
done for !--- users in a group called "eap_methods" who
use server group "rad_eap". . . . ! bridge irb !
interface Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
12345678901234567890123456 transmit-key !This step is
optional----!--- This value seeds the initial key for
use with !--- broadcast [255.255.255.255] traffic. If
more than one VLAN is !--- used, then keys must be set
for each VLAN. encryption vlan 1 mode wep mandatory !---
```

```
This defines the policy for the use of Wired Equivalent
Privacy (WEP). !--- If more than one VLAN is used, !---
the policy must be set to mandatory for each VLAN.
broadcast-key vlan 1 change 300 !--- You can also enable
Broadcast Key Rotation for each vlan and Specify the
time after which Brodacst key is changed. If it is
disabled Broadcast Key is still used but not changed.
ssid cisco vlan 1 !--- Create a SSID Assign a vlan to
this SSID authentication open eap eap_methods
authentication network-eap eap_methods !--- Expect that
users who attach to SSID "cisco" !--- request
authentication with the type 128 Open EAP and Network
EAP authentication !--- bit set in the headers of those
requests, and group those users into !--- a group called
"eap_methods." ! speed basic-1.0 basic-2.0 basic-5.5
basic-11.0 rts threshold 2312 channel 2437 station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled . . .
interface FastEthernet0 no ip address no ip route-cache
duplex auto speed auto bridge-group 1 no bridge-group 1
source-learning bridge-group 1 spanning-disabled !
interface BVI1 ip address 10.77.244.194 255.255.255.0 !-
-- The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.77.244.194 key shared_secret !---
Identifies itself as a RADIUS server, reiterates !---
"localness" and defines the key between the server
(itself) and the access point. ! group testuser !---
Groups are optional. ! user user1 nthash password1 group
testuser !--- Individual user user user2 nthash
password2 group testuser !--- Individual user !--- These
individual users comprise the Local Database ! radius-
server host 10.77.244.194 auth-port 1812 acct-port 1813
key shared_secret !--- Defines where the RADIUS server
is and the key between !--- the access point (itself)
and the server. radius-server retransmit 3 radius-server
attribute 32 include-in-access-req format %h radius-
server authorization permit missing Service-Type radius-
server vsa send accounting bridge 1 route ip ! ! line
con 0 line vty 5 15 ! end
```

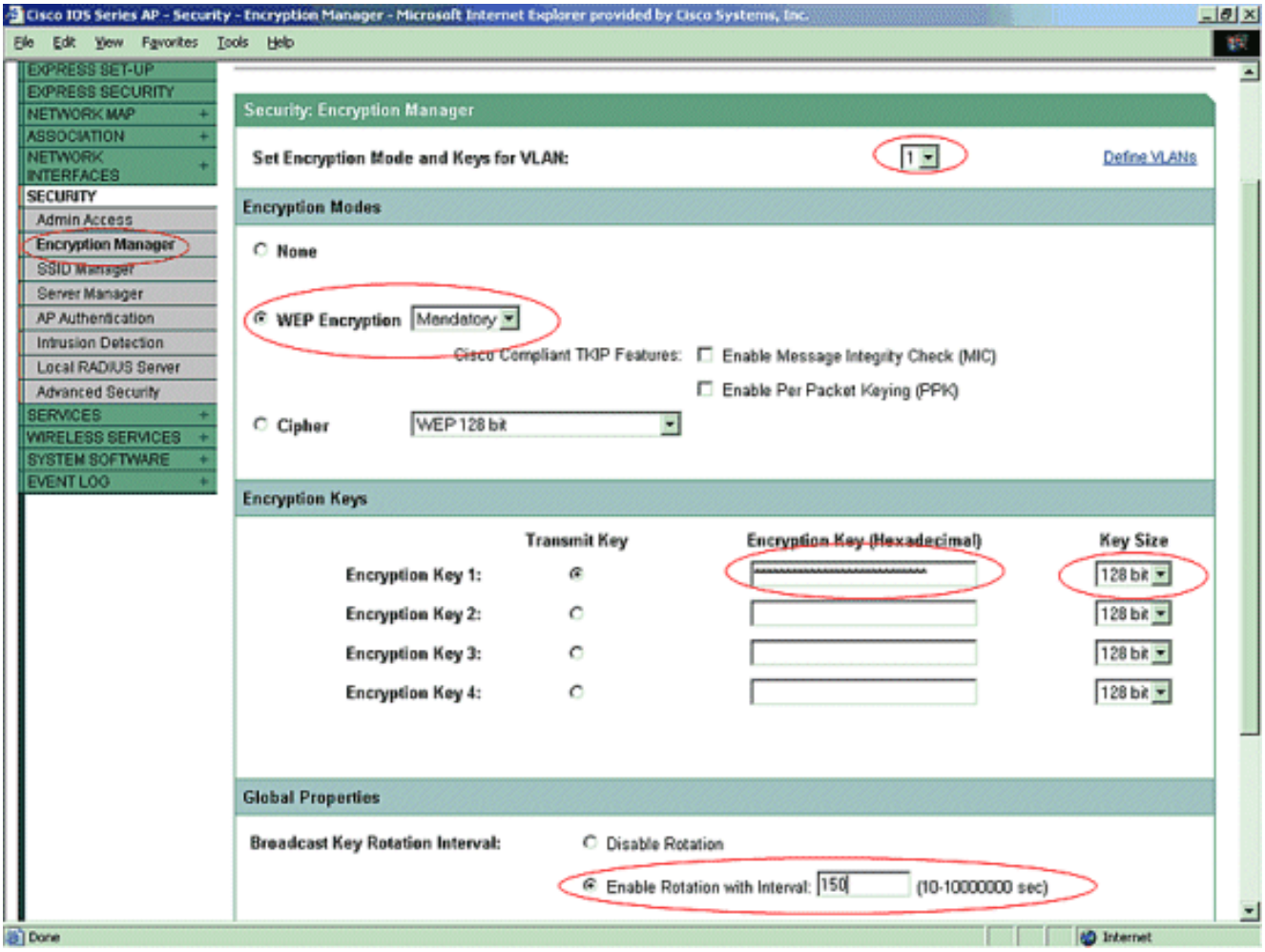
GUI 配置

完成以下步骤以通过 GUI 来配置本地 RADIUS 服务器功能：

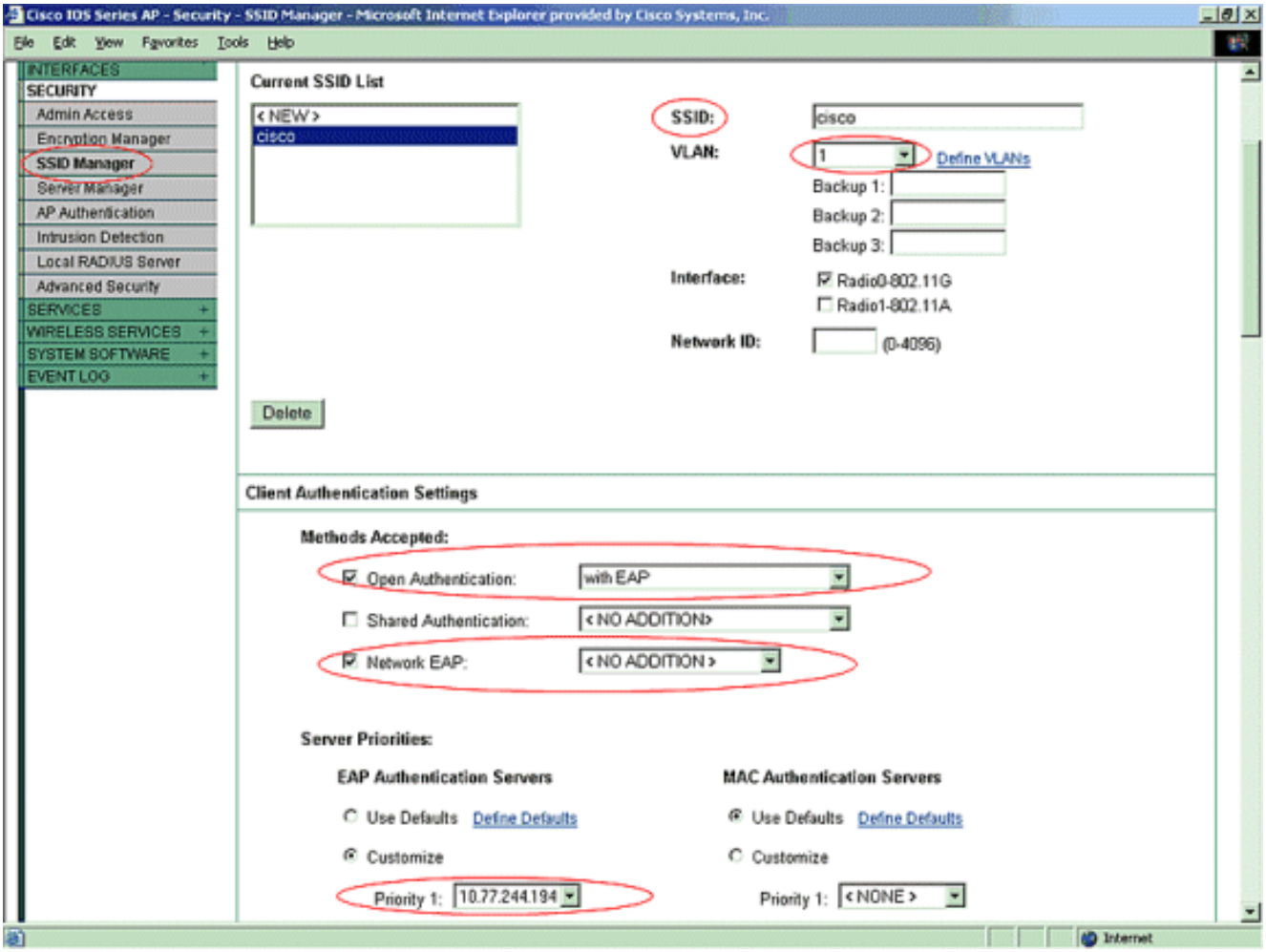
1. 在左侧菜单中的“Security”菜单下，选择“Server Manager”选项卡。配置服务器并输入此接入点的 IP 地址，本例中 IP 地址为 10.77.244.194。输入本地 Radius 服务器所侦听的端口号 1812 和 1813。指定要用于本地 RADIUS 服务器的共享密钥，如图显示。



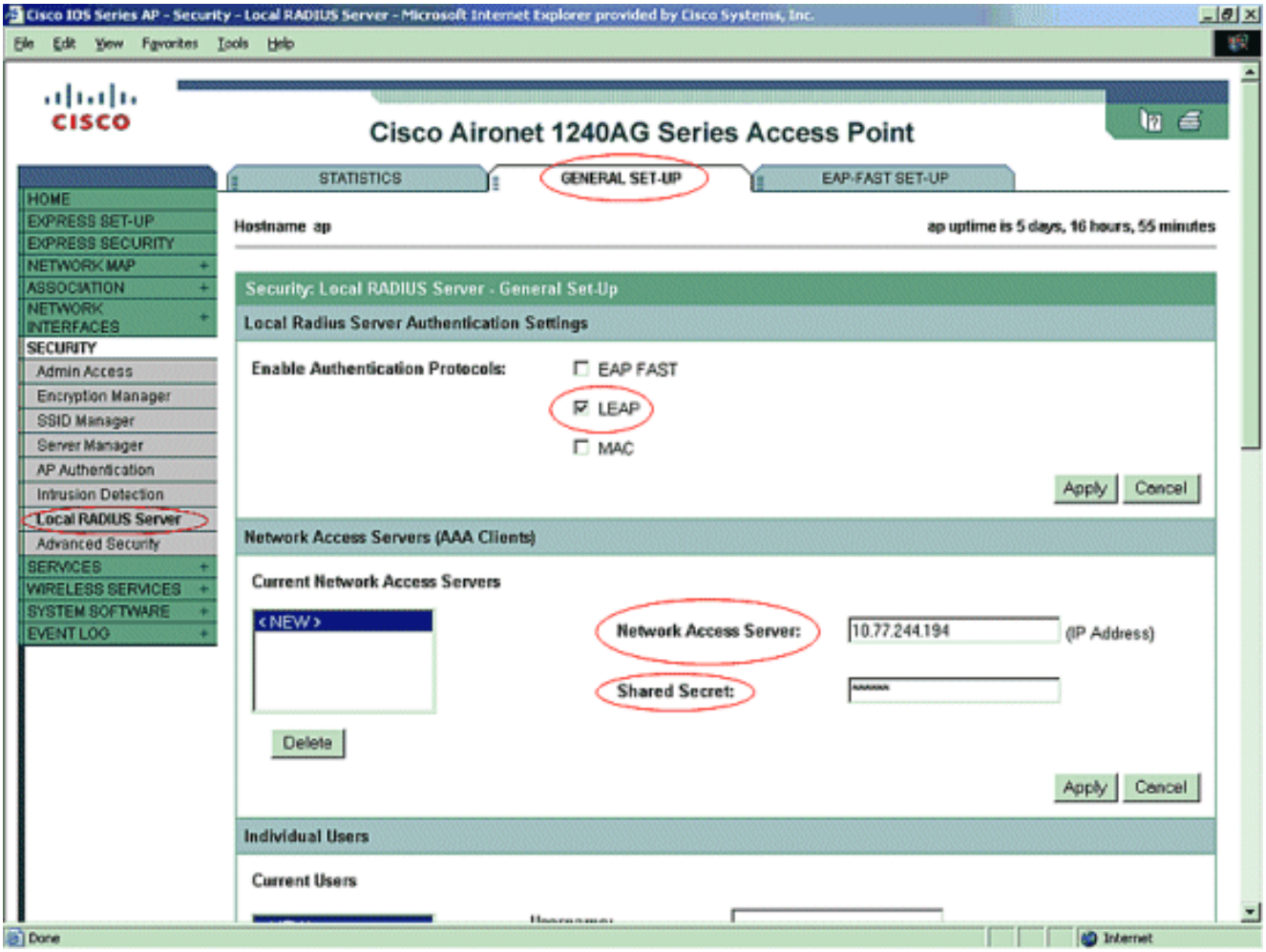
2. 在左侧菜单中的“Security”菜单下，单击“Encryption Manager”选项卡。指定要应用的 VLAN。指定将使用 WEP 加密。指定该加密是强制性的 (Mandatory)。用一个 26 位的十六进制字符对任何 WEP 密钥进行初始化。此密钥用于加密广播和组播数据包。此步骤是可选的。将密钥大小设置为 128 位。也可选择 40 位。在这种情况下，上一步中的 WEP 密钥大小必须是一个 10 位的十六进制字符。此步骤是可选的。也可启用广播密钥交替并指定更改广播密钥之前的时间。如果将广播密钥禁用，则该密钥仍可使用，但无法更改。此步骤是可选的。**注意**： 每个使用 LEAP 身份验证的 VLAN 都将重复这些步骤。单击 **Apply**。



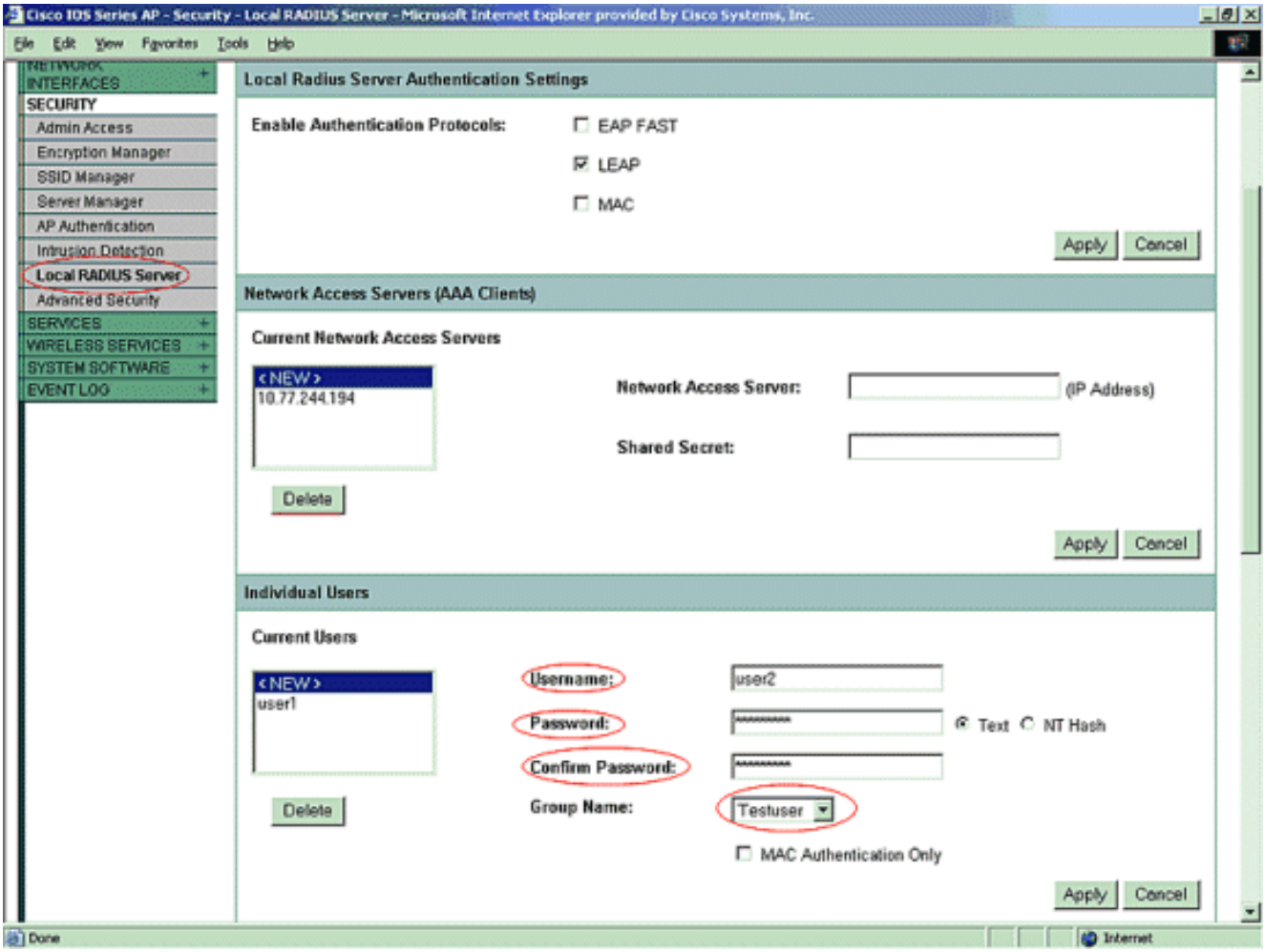
3. 从“Security”菜单下的“SSID Manager”选项卡执行以下操作：**注意：** 在您确认基本配置正确运行之后，随后可以添加其他功能和密钥管理。定义新的 SSID 并将其与一个 VLAN 相关联。在本示例中，该 SSID 与 VLAN 1 相关联。选中 **Open Authentication (With EAP)**。选中 **Network EAP (No Addition)**。从 **Server Priorities > EAP Authentication Servers** 中，选择 **Customize**；针对 **Priority 1** 选择此接入点的 IP 地址。单击 **Apply**。



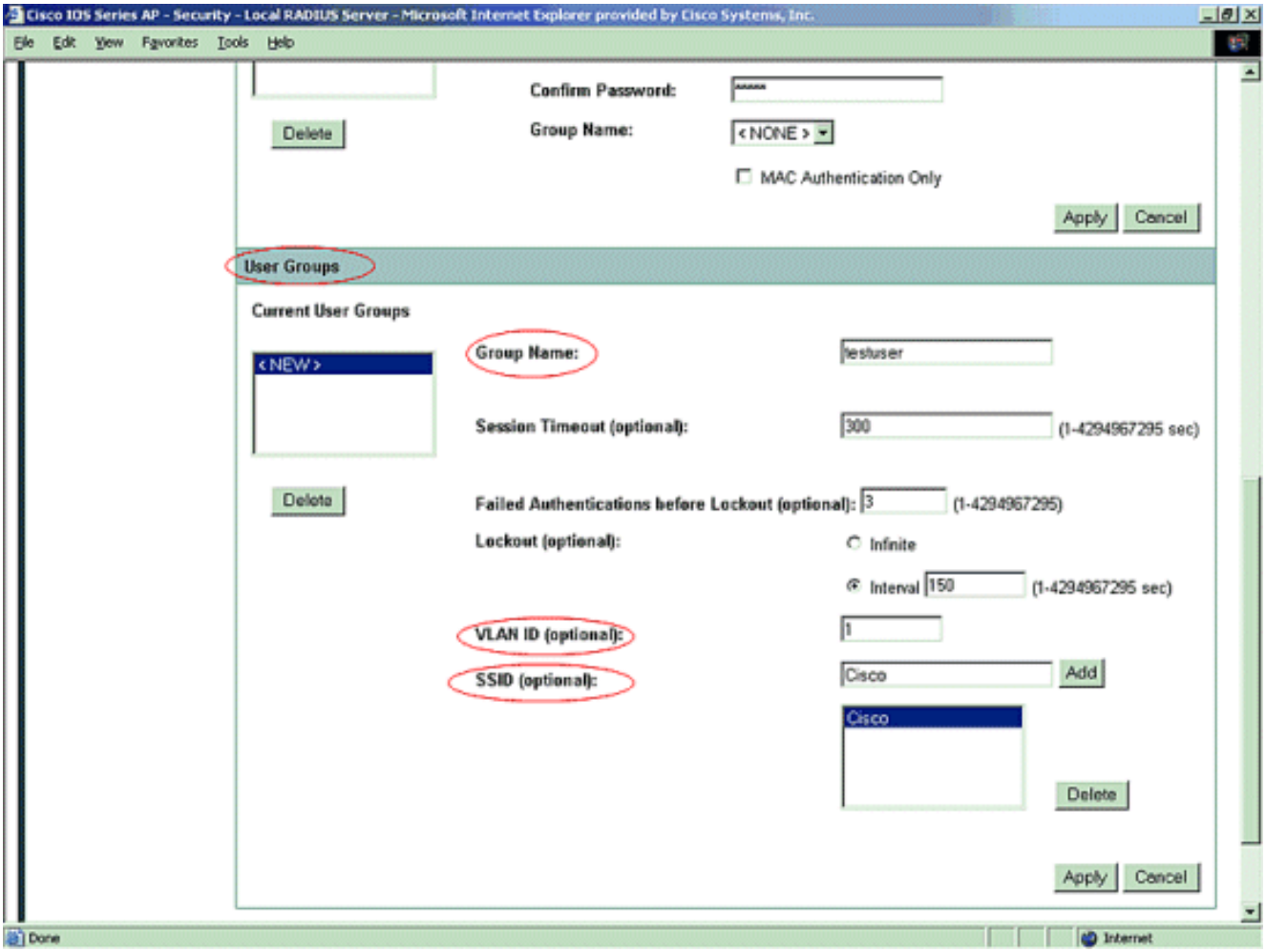
4. 在“Security”下面，从“General Set-UP”选项卡单击“Local RADIUS Server”。在“Local Radius Server Authentication Settings”下，选中 **LEAP** 以确保接受 LEAP 身份验证请求。定义 RADIUS 服务器的 IP 地址和共享密钥。对于本地 RADIUS 服务器，此地址为该 AP 的 IP 地址 (10.77.244.194)。单击 **Apply**。



5. 从“General Setup”选项卡中的“Local RADIUS Server”向下滚动，并定义各用户的用户名和口令。或者，可将用户与下一步中定义的组进行关联。这样就可确保只有某些用户可以登录到 SSID 中。**注意：** 本地 RADIUS 数据库由这些单独的用户名和口令组成。



6. 同样，从“General Set-Up”子选项卡中的“Local RADIUS Server”，在同一页上进一步向下滚动至“User Groups”；定义用户组并将其与 VLAN 或 SSID 相关联。



注意： 组是可选的。组属性不会传递到 Active Directory，并且是只与本地相关。您可以在您确认基本配置正常工作之后再添加组。

验证

使用本部分可确认配置能否正常运行。

- **show radius local-server statistics** - 此命令显示本地身份验证器所收集的统计信息。

```
Successes              : 27          Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.77.244.194
Successes              : 27          Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
Auto provision success : 0           Auto provision failure : 0
PAC refresh            : 0           Invalid PAC received   : 0

Username                  Successes  Failures  Blocks
user1                            27         0       0
```

- **show radius server-group all** - 此命令显示接入点上所有已配置的 RADIUS 服务器组的列表。

故障排除

故障排除步骤

此部分提供故障排除信息与此配置有关。

1. 为了消除可能发生的可阻止成功身份验证的 RF 问题，请将 SSID 上的方法设置为 **Open**，以临时禁用身份验证。从 GUI - 在“SSID Manager”页上，取消选中 **Network-EAP**，然后选中 **Open**。从命令行 - 使用命令 **authentication open** 和 **no authentication network-eap eap_methods**。如果客户端成功关联，则 RF 与关联问题无关。
2. 验证所有共享密钥口令是否同步。线路RADIUS服务器主机x.x.x.x auth端口x acct-port x密钥< shared_secret >和NAS x.x.x.x密钥< shared_secret >，必须包含相同的共享秘密密码。
3. 删除所有用户组和用户组相关配置。有时，在接入点定义的用户组与域上的用户组之间可能会发生冲突。

故障排除命令

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug dot11 aaa authenticator all** - 此调试会显示某个客户端通过 802.1x 或 EAP 进程进行关联和身份验证时，从身份验证器（接入点）的角度经历的各种协商。这个debug在Cisco IOS软件版本12.2(15)JA介绍过。此命令在该版本和更高版本中会废弃 debug dot11 aaa dot1x all。

```
 *Mar  1 00:26:03.097: dot11_auth_add_client_entry:
   Create new client 0040.96af.3e93 for application 0x1
 *Mar  1 00:26:03.097: dot11_auth_initialize_client:
   0040.96af.3e93 is added to the client list for application 0x1
-----------------------------------------------
   Lines Omitted for simplicity ------------------
*Mar  1 00:26:03.098: dot11_auth_dot1x_start:
   in the dot11_auth_dot1x_start


*Mar  1 00:26:03.132: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93
*Mar  1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client:
   Sending identity request to 0040.96af.3e93(client) *Mar 1 00:26:03.133: *Mar 1
00:26:03.099: dot11_auth_dot1x_send_id_req_to_client: Client 0040.96af.3e93 timer started
for 30 seconds *Mar 1 00:26:03.132: dot11_auth_parse_client_pak: Received EAPOL packet from
0040.96af.3e93 ----------------------------------------------- Lines Omitted---------------
------------------- *Mar 1 00:26:03.138: EAP code: 0x2 id: 0x1 length: 0x000A type: 0x1
01805BF0: 0100000A 0201000A 01757365 7231 .........user1(User Name of the client) *Mar1
00:26:03.146: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY) for
0040.96af.3e93 *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server: Sending client
0040.96af.3e93 data to server *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds ------------------------------------------------
Lines Omitted---------------------------------- *Mar1 00:26:03.150:
dot11_auth_dot1x_parse_aaa_resp: Received server response:GET_CHALLENGE_RESPONSE *Mar1
00:26:03.150: dot11_auth_dot1x_parse_aaa_resp: found session timeout 10 sec *Mar 1
00:26:03.150: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_REPLY) for
0040.96af.3e93 *Mar 1 00:26:03.150: dot11_auth_dot1x_send_response_to_client: Forwarding
server message to client 0040.96af.3e93 ------------------------------------------- Lines
Omitted------------------------------------ *Mar 1 00:26:03.151: dot11_auth_send_msg:
Sending EAPOL to requestor *Mar 1 00:26:03.151: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 10 seconds *Mar 1 00:26:03.166: dot11_auth_parse_client_pak:
Received EAPOL packet(User Credentials) from 0040.96af.3e93 *Mar 1 00:26:03.166: EAP code:
0x2 id: 0x11 length: 0x0025 type: 0x11 01805F90: 01000025 02110025...%...%01805FA0: 11010018
7B75E719 C5F3575E EFF64B27 ....{ug.EsW^ovK' Executing Action(CLIENT_WAIT,CLIENT_REPLY) for
0040.96af.3e93 *Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: Sending client
0040.96af.3e93 data (User Credentials) to server *Mar 1 00:26:03.186:
```

dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds ----------
---------- Lines Omitted----------
*Mar 1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp: **Received server response: PASS** *Mar 1 00:26:03.197: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93 *Mar 1 00:26:03.197: dot11_auth_dot1x_send_response_to_client: **Forwarding server message*(Pass Message)* to client** ----------
Lines Omitted---------- *Mar 1 00:26:03.198: dot11_auth_send_msg: Sending EAPOL to requestor *Mar 1 00:26:03.199: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 second *Mar 1 00:26:03.199: dot11_auth_send_msg: **client authenticated 0040.96af.3e93,** node_type 64 for application 0x1 *Mar 1 00:26:03.199: dot11_auth_delete_client_entry: 0040.96af.3e93 is deleted for application 0x1 *Mar 1 00:26:03.200: %DOT11-6-ASSOC: **Interface Dot11Radio0, Station *Station Name* 0040.96af.3e93 Associated KEY_MGMT[NONE]**

- debug radius authentication - 此调试显示服务器与客户端之间的 RADIUS 协商，此时两者均为接入点。
- debug radius local-server client - 此调试从 RADIUS 服务器的角度显示客户端的身份验证。

*Mar 1 00:30:00.742: RADIUS(0000001A):
Send Access-Request*(Client's User Name)* to 10.77.244.194:1812*(Local Radius Server)* id 1645/65, len 128 *Mar 1 00:30:00.742: RADIUS: **User-Name [1] 7 "user1"** *Mar 1 00:30:00.742: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0" *Mar 1 00:30:00.743: RADIUS: **Calling-Station-Id [31] 16 "0040.96af.3e93" *(Client)*** *Mar 1 00:30:00.743: RADIUS: Service-Type [6] 6 Login [1] *Mar 1 00:30:00.743: RADIUS: Message-Authenticato[80] *Mar 1 00:30:00.743: RADIUS: 23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B [#.?B??rK(DnzX??{] *Mar 1 00:30:00.743: RADIUS: EAP-Message [79] 12 *Mar 1 00:30:00.743: **RADIUS: 02 02 00 0A 01 75 73 65 72 31 [?????user1]** *Mar 1 00:30:00.744: RADIUS: NAS-Port-Type [61] 6 802.11 wireless ----------
---------- Lines Omitted For Simplicity---------- *Mar 1 00:30:00.744: RADIUS: **NAS-IP-Address [4] 6 10.77.244.194*(Access Point IP)*** *Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap" ---------- Lines Omitted----------
---------- *Mar 1 00:30:00.745: RADIUS: **Received from id 1645/65 10.77.244.194:1812, Access-Challenge**, len 117 *Mar 1 00:30:00.746: RADIUS: 75 73 65 72 31 **[user1]** *Mar 1 00:30:00.746: RADIUS: Session-Timeout [27] 6 10 *Mar 1 00:30:00.747: RADIUS: State [24] 50 *Mar 1 00:30:00.747: RADIUS: BF 2A A0 7C 82 65 76 AA 00 00 00 00 00 00 00 00 [?*?|?ev?????????] ---------- Lines Omitted for simplicity ----
--------- *Mar 1 00:30:00.756: RADIUS/ENCODE(0000001A):Orig. component type = DOT11 *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: ssid [264] 5 *Mar 1 00:30:00.756: RADIUS: 63 69 73 [cis] *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: interface [157] 3 *Mar 1 00:30:00.756: RADIUS: 32 [2] *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A): acct_session_id: 26 *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.779: RADIUS(0000001A): **Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189** *Mar 1 00:30:00.779: RADIUS: authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F *Mar 1 00:30:00.779: RADIUS: User-Name [1] 7 "user1" *Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400 *Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0" *Mar 1 00:30:00.780: RADIUS: Calling-Station-Id [31] 16"0040.96af.3e93" *Mar 1 00:30:00.758: RADIUS: 92 D4 24 49 04 C2 D2 0A C3 CE E9 00 6B F1 B2 AF [??$I????????k???] *Mar 1 00:30:00.759: RADIUS: EAP-Message [79] 39 *Mar 1 00:30:00.759: RADIUS: 02 17 00 25 11 01 00 18 05 98 8B BE 09 E9 45 E2 **[??????????????E?**] *Mar 1 00:30:00.759: RADIUS: 73 5D 33 1D F0 2F DB 09 50 AF 38 9F F9 3B BD D4 **[s]3??/??P?8??;??]** *Mar 1 00:30:00.759: RADIUS: 75 73 65 72 31 [user1] ---------- Lines Omitted----------
*Mar 1 00:30:00.781: RADIUS: State [24] 50 RADIUS: NAS-IP-Address [4] 6 10.77.244.194 *Mar 1 00:30:00.783: RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 00:30:00.822: RADIUS: **Received from id 1645/67 10.77.244.194:1812, Access-Accept, len 214** *Mar 1 00:30:00.822: RADIUS: authenticator 10 0C B6 EE 7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A ----------
---------- Lines Omitted---------- *Mar 1 00:30:00.823: RADIUS: 75 73 65 72 31 [user1] *Mar 1 00:30:00.823: RADIUS: Vendor, Cisco [26] 59 *Mar 1 00:30:00.823: RADIUS: Cisco AVpair [1] 53 **"leap:session-key=?+*ve=];q,oi[d6|-z."** *Mar 1 00:30:00.823: RADIUS: User-Name [1] 28 "user1 *Mar 1 00:30:00.824: RADIUS: Message-Authenticato[80] 18 *Mar 1 00:30:00.824: RADIUS: 06 2D BA 93 10 C0 91 F8 B4 B8 A4 00 82 0E 11 36 [?-????????????6] *Mar 1 00:30:00.826: RADIUS/DECODE: EAP-Message fragments, 37, total 37 bytes *Mar 1 00:30:00.826: **found leap session key** *Mar 1 00:30:00.830: %DOT11-6-ASSOC: **Interface Dot11Radio0, Station *Station Name* Associated KEY_MGMT[NONE]**

- debug radius local-server packets - 此调试从 RADIUS 服务器的角度显示其完成的所有进程。

相关信息

- 将接入点配置为本地身份验证器
- 配置身份验证类型
- 配置 RADIUS 和 TACACS+ 服务器
- 技术支持和文档 - Cisco Systems