在一个本地RADIUS服务器的LEAP认证

Contents

Introduction

本文为轻量级扩展身份认证协议(LEAP)认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。这是可适用的对运行12.2(11)JA或以上的IOS接入点。

Prerequisites

Requirements

尝试进行此配置之前，请确保满足以下要求：

- 与IOS GUI或CLI的熟悉
- 与概念的熟悉在LEAP认证后

组件

本文档中的信息基于以下软件和硬件版本。

- Cisco Aironet 1240AG系列访问访问接入点
- Cisco IOS Software Release 12.3(8)JA2
- Cisco Aironet运行Aironet Desktop软件3.6.0.122的802.11 a/b/g/无线适配器
- 仅在网络的一个VLAN的做法

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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

本地RADIUS服务器功能概述

通常一个外部RADIUS服务器用于验证用户。有时，这不是一个可行解决方案。在这些情况下，接入点可以被做作为RADIUS服务器。这里，用户利用在接入点配置的本地数据库验证。这称为一个本地RADIUS服务器功能。您能也做在本地RADIUS服务器在接入点以为特色的网络使用的其他接入点。关于此的更多信息，请参见配置其他接入点使用本地证明人。

Configure

配置描述如何配置LEAP和本地RADIUS服务器功能在接入点。本地RADIUS服务器功能在Cisco IOS Software Release 12.2(11)JA被介绍了。参考LEAP认证用RADIUS服务器关于如何的背景信息用一个外部RADIUS服务器配置LEAP。

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。您必须创建强口令策略减轻词典攻击，那将包括严格的密码并且常去新的密码。参考对Cisco LEAP的词典攻击关于词典攻击的更多信息和如何防止他们。

本文采取CLI和GUI的此配置：

1. 接入点的IP地址是**10.77.244.194**。
2. 使用的SSID是**cisco**，被映射对**VLAN 1**。
3. 用户名是**user1**和**user2**，被映射对组**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
```

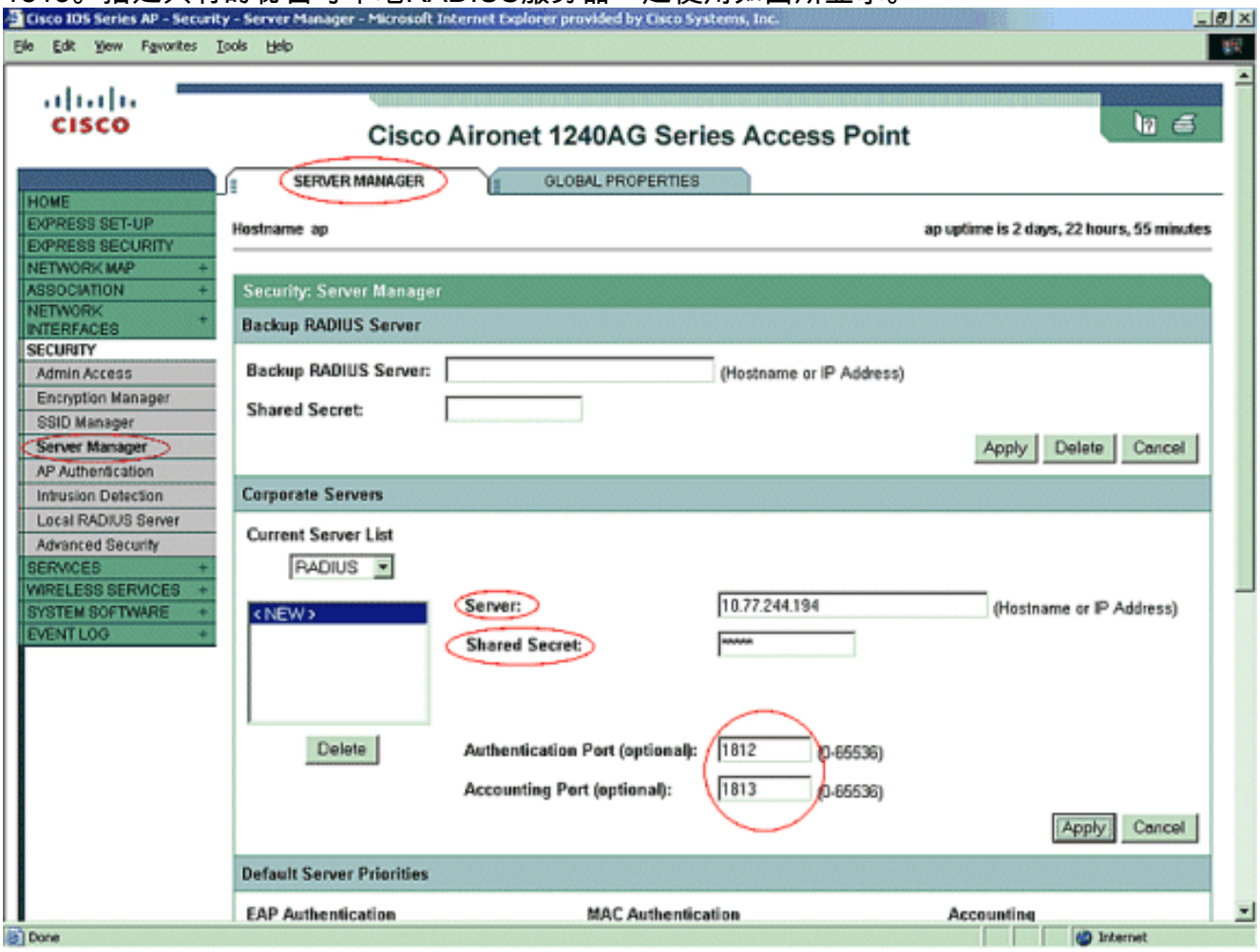
```
   12345678901234567890123456 transmit-key
!This step is optional----!--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory !--- This defines the policy
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
```

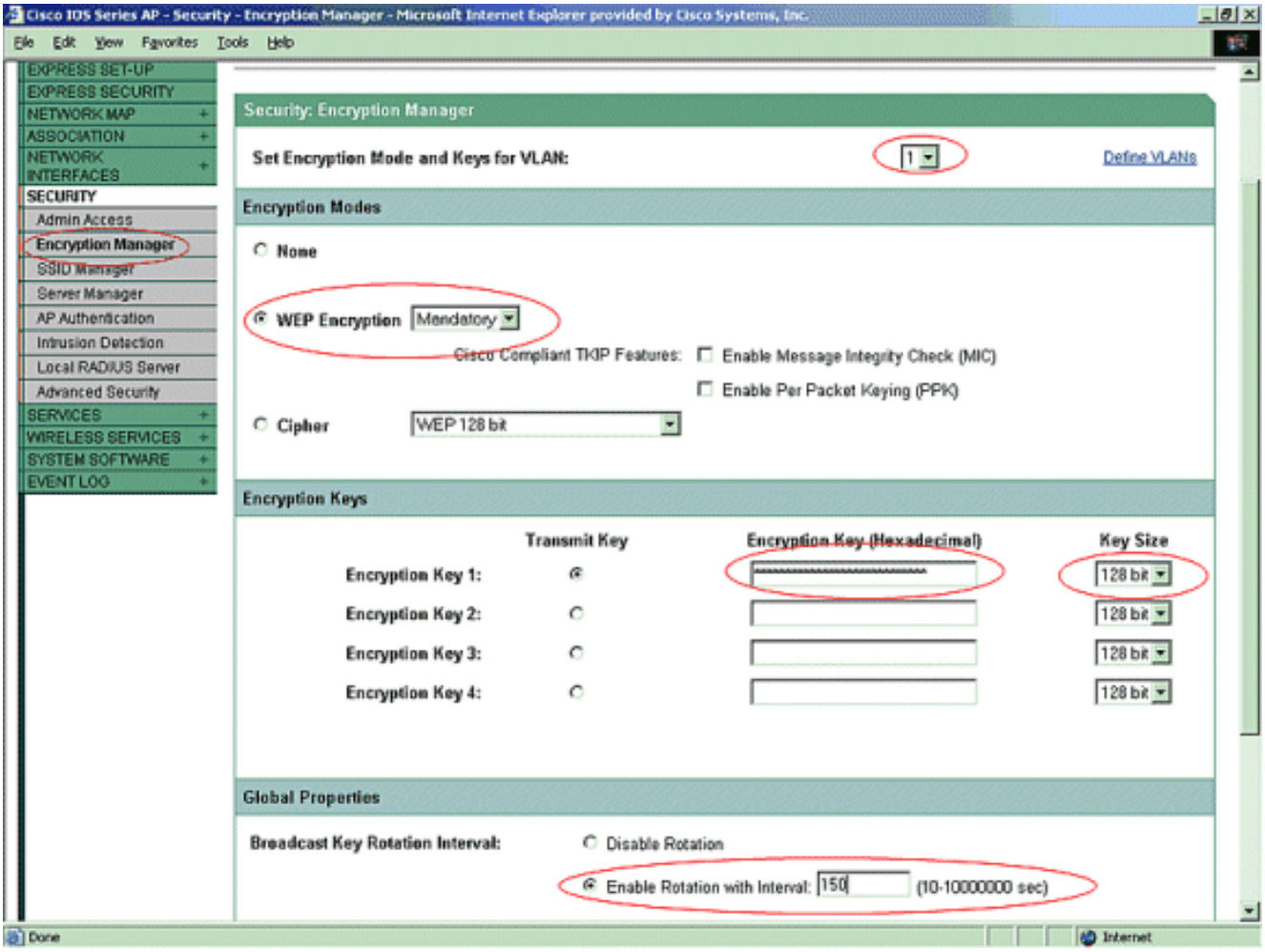
GUI 配置

完成这些步骤为了用GUI配置本地RADIUS服务器功能：

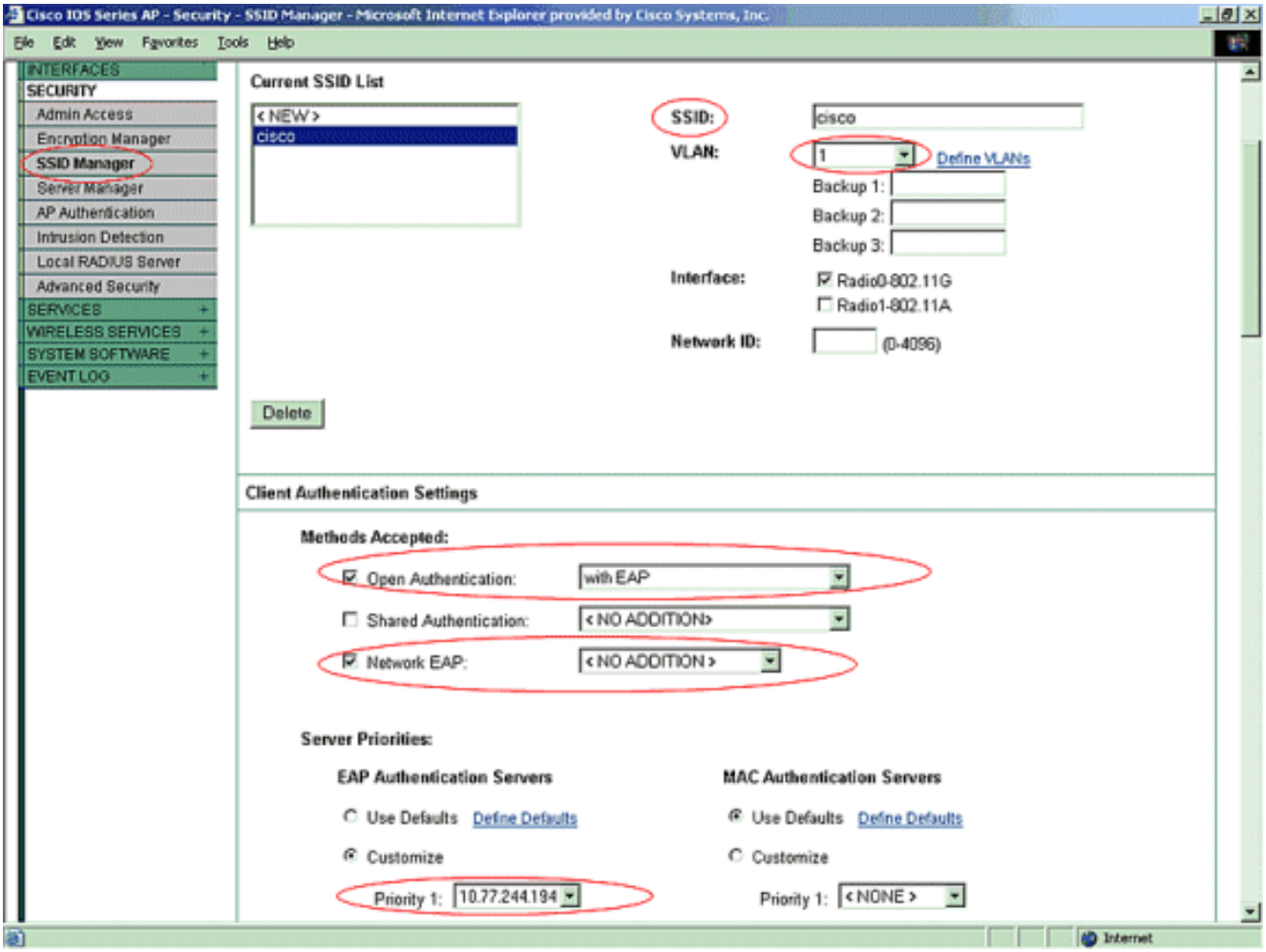
1. 从在左手边的菜单，请选择Server Manager选项在Security菜单下。配置服务器并且提及此接入点的IP地址，是在本例中的10.77.244.194。提及端口号本地RADIUS服务器监听的1812和1813。指定共有的秘密与本地RADIUS服务器一起使用如图所示。



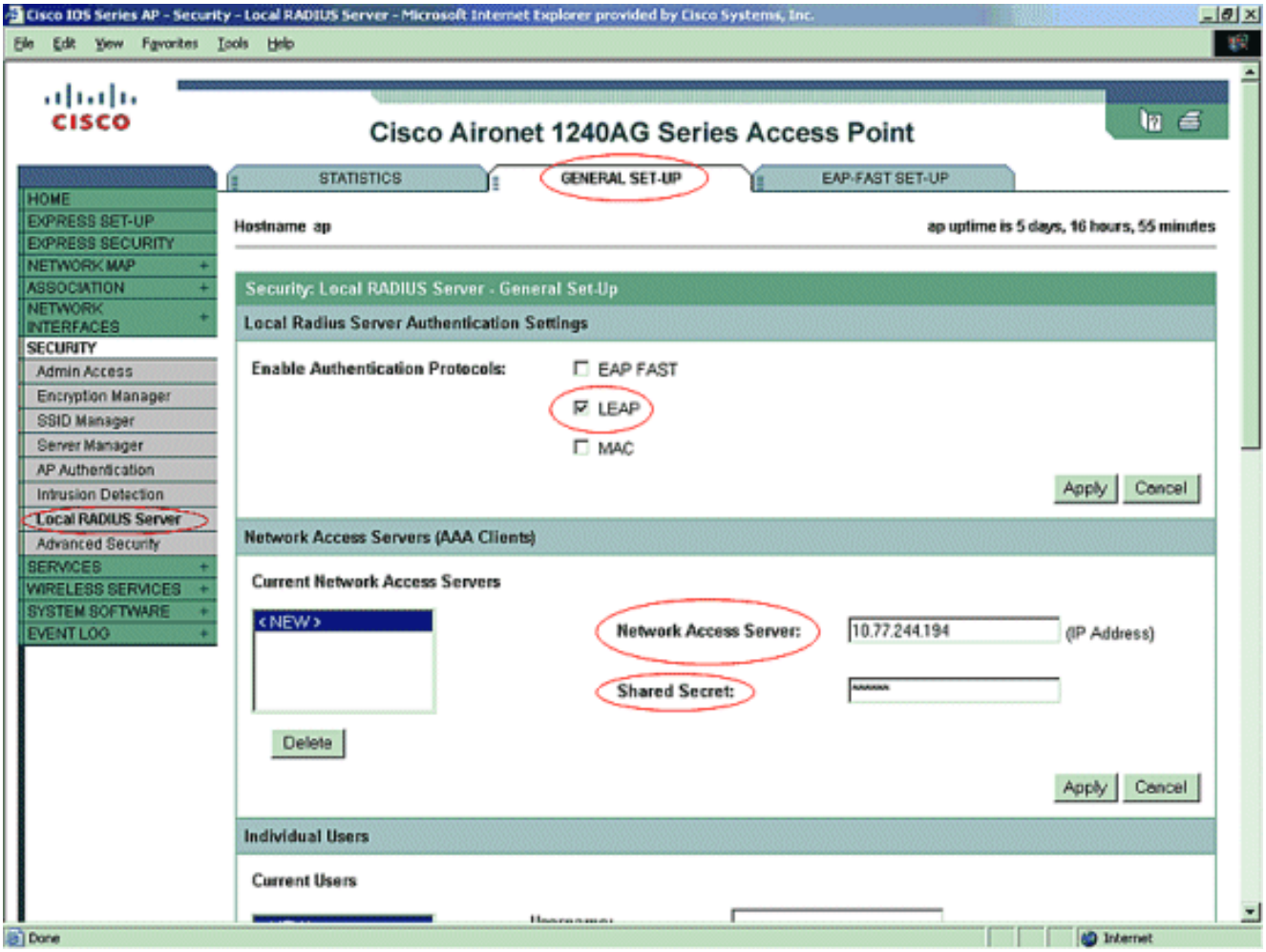
2. 从在左手边的菜单，请点击Encryption Manager选项在Security菜单下。指定将适用的VLAN。指定将使用WEP加密。指定其使用是MANDATORY。初始化与26位十六进制字符的所有WEP密钥。此键用于加密广播和组播信息包。此步骤是可选的。设置密钥大小为128位。您能也选择40位。在这种情况下，在上一步的WEP密钥大小必须是10位十六进制字符。此步骤是可选的。您也能enable (event)广播密钥交替和指定时间，在后更换广播键。如果它是失效的，仍然使用广播键，但是没有被更换。此步骤是可选的。**Note:** 这些步骤为使用LEAP认证的每个VLAN被重复单击 **Apply**。



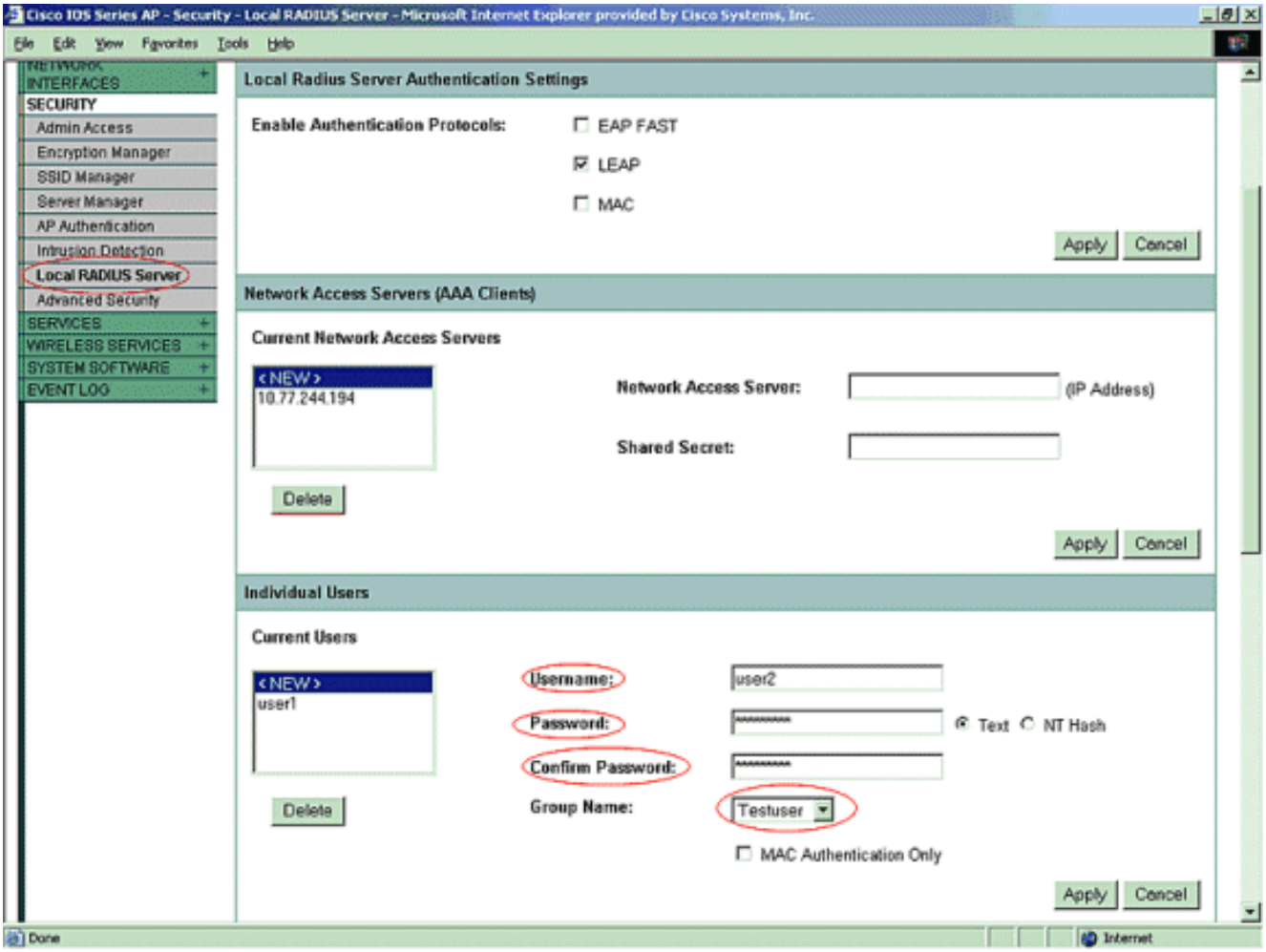
3. 在Security菜单下，从SSID Manager选项，请进行这些动作：**Note:** 您能后添加其它功能和密钥管理，一旦确认基本配置正确地工作。定义一新的SSID并且连结它与VLAN。在本例中，SSID与VLAN 1.产生关联。检查**开放式验证(与EAP)**。检查**网络EAP (没有添加)**。从**服务器优先级> EAP认证服务器**，请选择**定制**;选择此接入点forPriority **1.的**IP地址**。**单击 **Apply**。



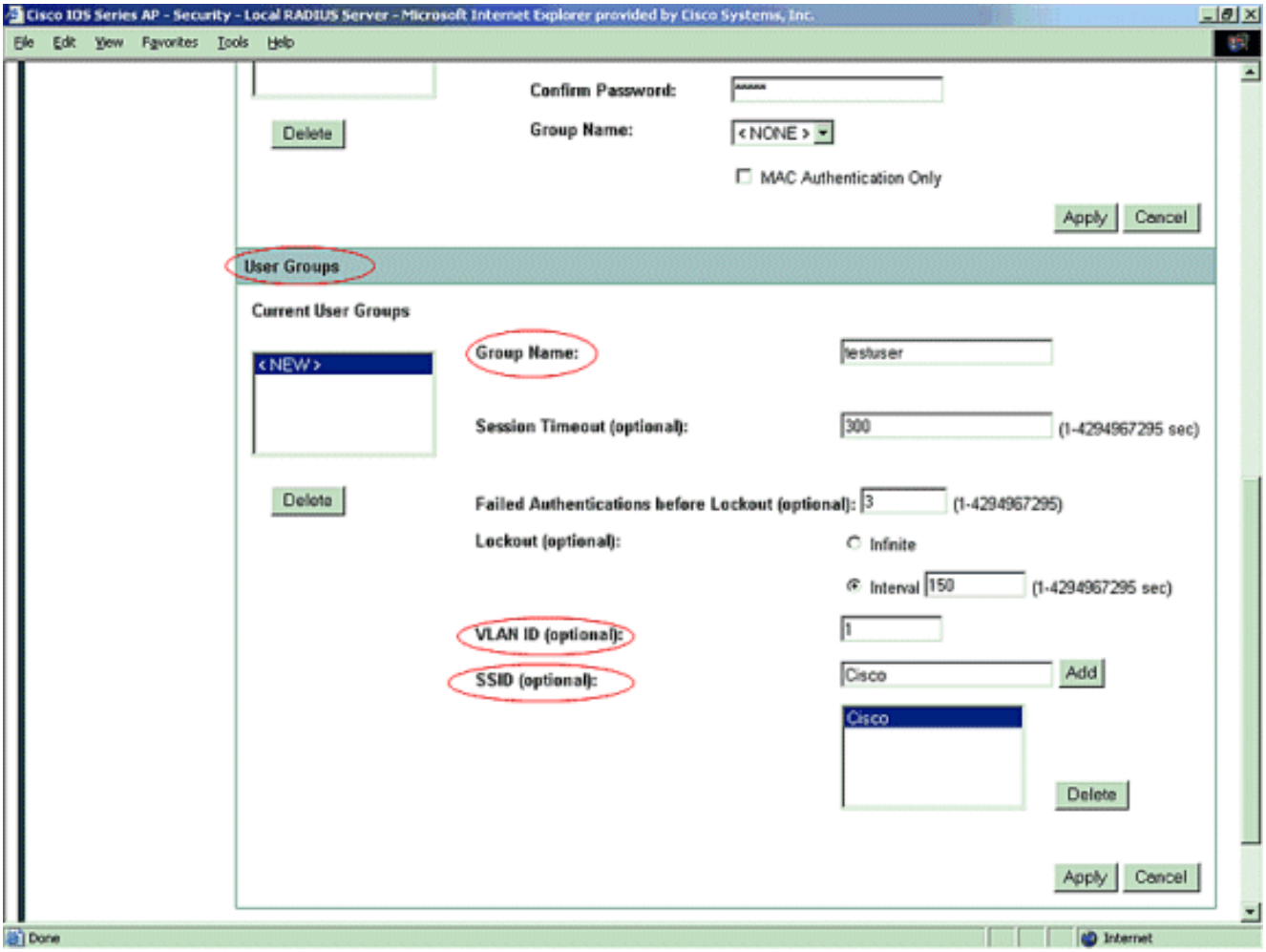
4. 在安全下，请点击从一般设置选项的本地RADIUS服务器在本地RADIUS服务器认证设置下，确信检查的**LEAP**， LEAP认证请求被接受。定义RADIUS服务器的IP地址和共有的秘密。对于本地RADIUS服务器，这是此AP (10.77.244.194)的IP地址。单击 **Apply**。



5. 从本地RADIUS服务器移下来在一般设置选项下并且定义有他们的用户名和密码的个人用户。随意地，用户可以被关联到组，在下一步被定义。这保证仅该某些用户日志到SSID。**Note:** 本地RADIUS数据库包括这些各自的用户名和密码。



6. 进一步移动下来在同一页，再从本地RADIUS服务器在一般设置sub选项下到用户组;定义用户组并且关联他们对VLAN或SSID。



Note: 组是可选的。组属性不通过对激活目录并且是只本地相关的。您能添加后组，一旦确认基本配置正确地工作。

Verify

Use this section to confirm that your configuration works properly.

- **show radius local-server statistics** —此命令显示本地证明人收集的统计数据。

```
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
   123456789012345678901234567890123456 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/help/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
```

- **全show radius的服务器组**此命令显示接入点的所有被配置的RADIUS服务器组列表。

Troubleshoot

故障检修程序

此部分提供故障排除信息与此配置有关。

1. 为了排除RF问题的可能性防止成功的验证的，请设置在SSID的方法**打开**临时地禁用认证。从GUI —在SSID管理器页，请不选定**网络EAP**并且检查**开放**。从line命令—请勿请使用authentication open命令和**authentication network-eap eap_methods**。如果客户端顺利地联合，RF不造成关联问题。
2. 验证所有共有的秘密密码同步。线路`RADIUSx.x.x.x authx acct-port x<shared_secret>`nas `x.x.x.x<shared_secret>`同一个共有的秘密密码。
3. 去除所有用户组和配置关于用户组。有时冲突能发生在域的接入点定义的用户组和用户组之间。

故障排除命令

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

- **调试全dot11 aaa的证明人**此调试表示多种协商，客户端经历，当客户端通过802.1x或EAP进程联合并且验证从证明人(接入点)的角度。此调试在Cisco IOS Software Release 12.2(15)JA被引入。此命令废弃debug dot11 aaa dot1x all由于及以后版本。

```
*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 toserver
*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


*Mar1 00:26:03.197: dot11_auth_dot1x_run_rfsm:
   ExecutingAction(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 —此调试显示在服务器和客户端之间的RADIUS协商，其中之二，在这种情况下，是接入点。
- debug radius local-server client —此调试从RADIUS服务器的角度显示客户端的认证。

```
 *Mar 1 00:30:00.742: RADIUS(0000001A):
   SendAccess-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 8265 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 100:30:00.756: 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 —此调试显示从RADIUS服务器的角度完成的由和所有进程
  。

Related Information

- 配置接入点作为一个本地证明人
- 配置身份验证类型
- 配置 RADIUS 和 TACACS+ 服务器
- Technical Support & Documentation - Cisco Systems