本地RADIUS伺服器上的LEAP驗證

目錄

簡介

本檔案將提供在基於IOS®的存取點上進行輕型可擴充驗證通訊協定(LEAP)驗證的範例組態，該存取點為無線使用者端提供服務，並充當本地RADIUS伺服器。這適用於執行12.2(11)JA或更新版本的IOS存取點。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 熟悉IOS GUI或CLI
- 熟悉LEAP身份驗證背後的概念

元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco Aironet 1240AG系列存取點
- Cisco IOS軟體版本12.3(8)JA2
- 運行Aironet案頭實用程式3.6.0.122的Cisco Aironet 802.11 a/b/g/無線介面卡
- 假設網路中只有一個VLAN

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

本地RADIUS伺服器功能概述

通常使用外部RADIUS伺服器來驗證使用者身分。在某些情況下，這不是一個可行的解決方案。在這些情況下，可以使接入點充當RADIUS伺服器。在這裡，使用者根據在接入點中配置的本地資料庫進行身份驗證。此功能稱為本地RADIUS伺服器功能。還可以使網路中的其他接入點使用接入點上的本地RADIUS伺服器功能。如需這方面的詳細資訊，請參閱設定其他存取點以使用本機驗證器。

設定

此配置描述如何在接入點上配置LEAP和本地Radius伺服器功能。本地RADIUS伺服器功能是在Cisco IOS軟體版本12.2(11)JA中匯入。有關如何使用外部RADIUS伺服器配置LEAP的後台資訊，請參閱使用RADIUS伺服器進行LEAP身份驗證。

與大多數基於密碼的身份驗證演算法一樣，Cisco LEAP容易受到字典攻擊。這不是Cisco LEAP的新攻擊或新漏洞。您必須建立強密碼策略來緩解字典攻擊，包括強密碼和頻繁使用的新密碼。請參閱Cisco LEAP上的字典攻擊，瞭解有關字典攻擊及其預防方法的詳細資訊。

本檔案將假設CLI和GUI的以下設定：

1. 接入點的IP地址為**10.77.244.194**。
2. 使用的SSID是**cisco**，對映到**VLAN 1**。
3. 使用者名稱是**user1**和**user2**，它們對映到組**Testuser**。

CLI組態

存取點

```
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 !
```

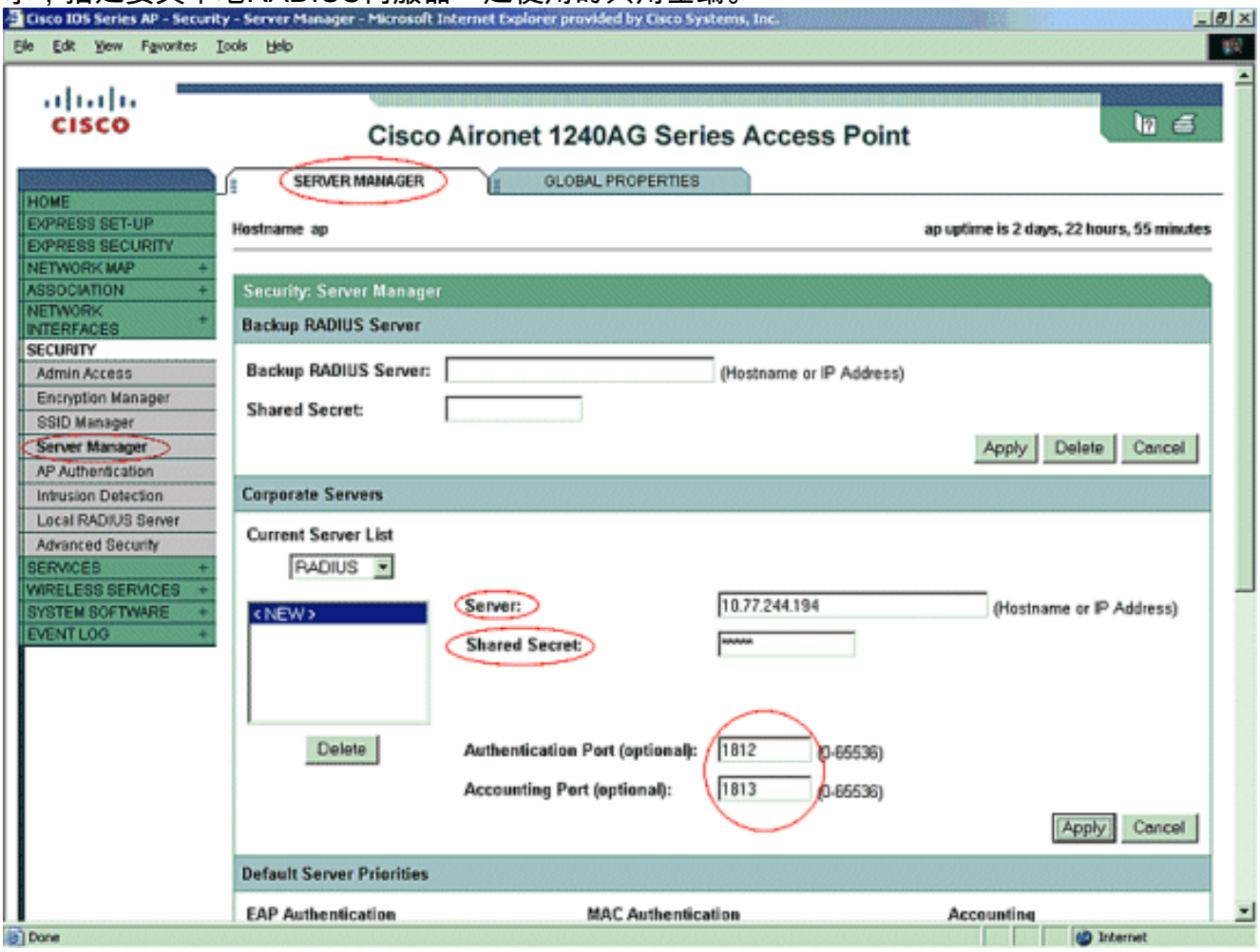
```
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!This step is optional----!--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep 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
```

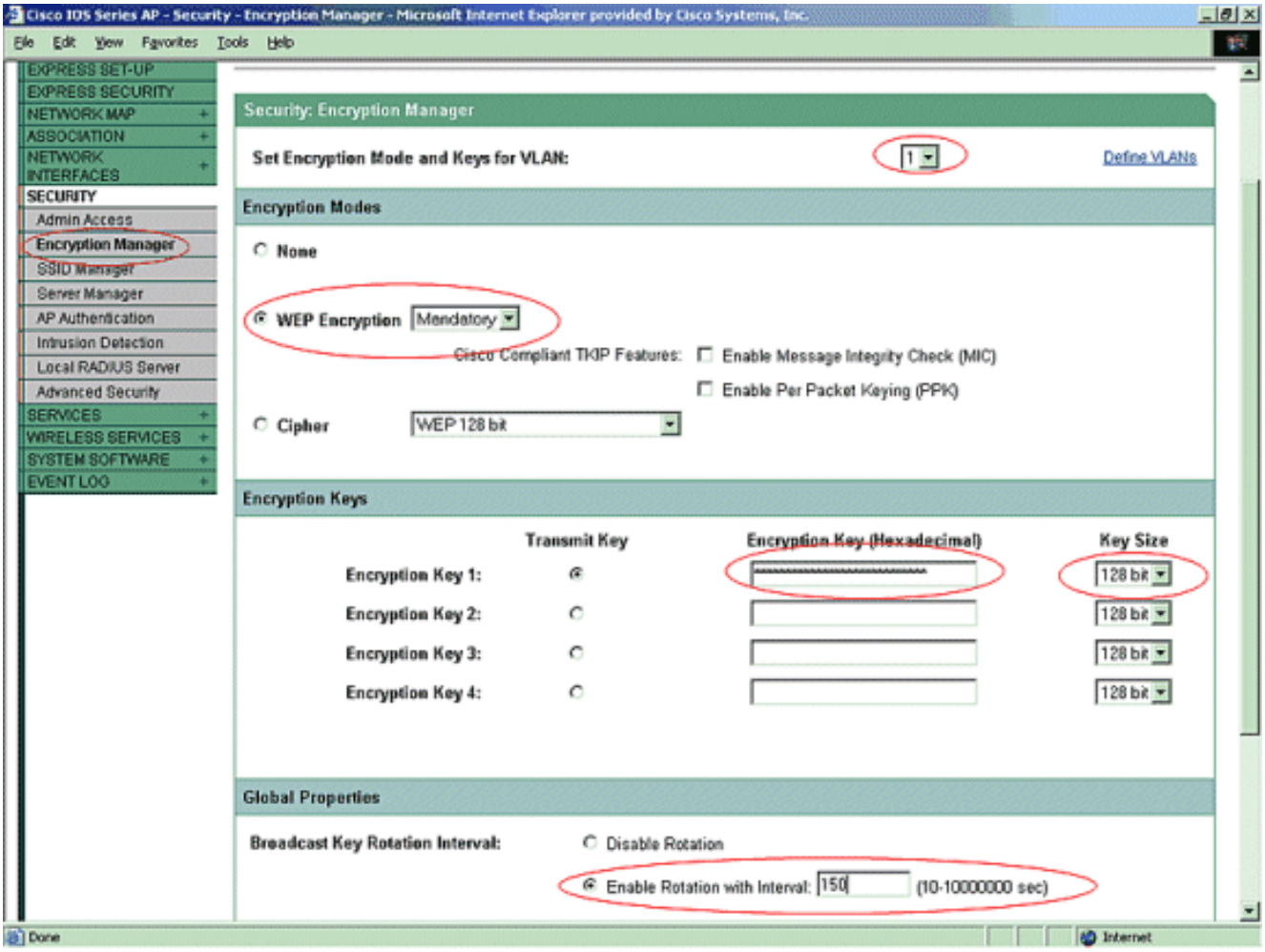
GUI配置

完成以下步驟，以便使用GUI設定本地RADIUS伺服器功能：

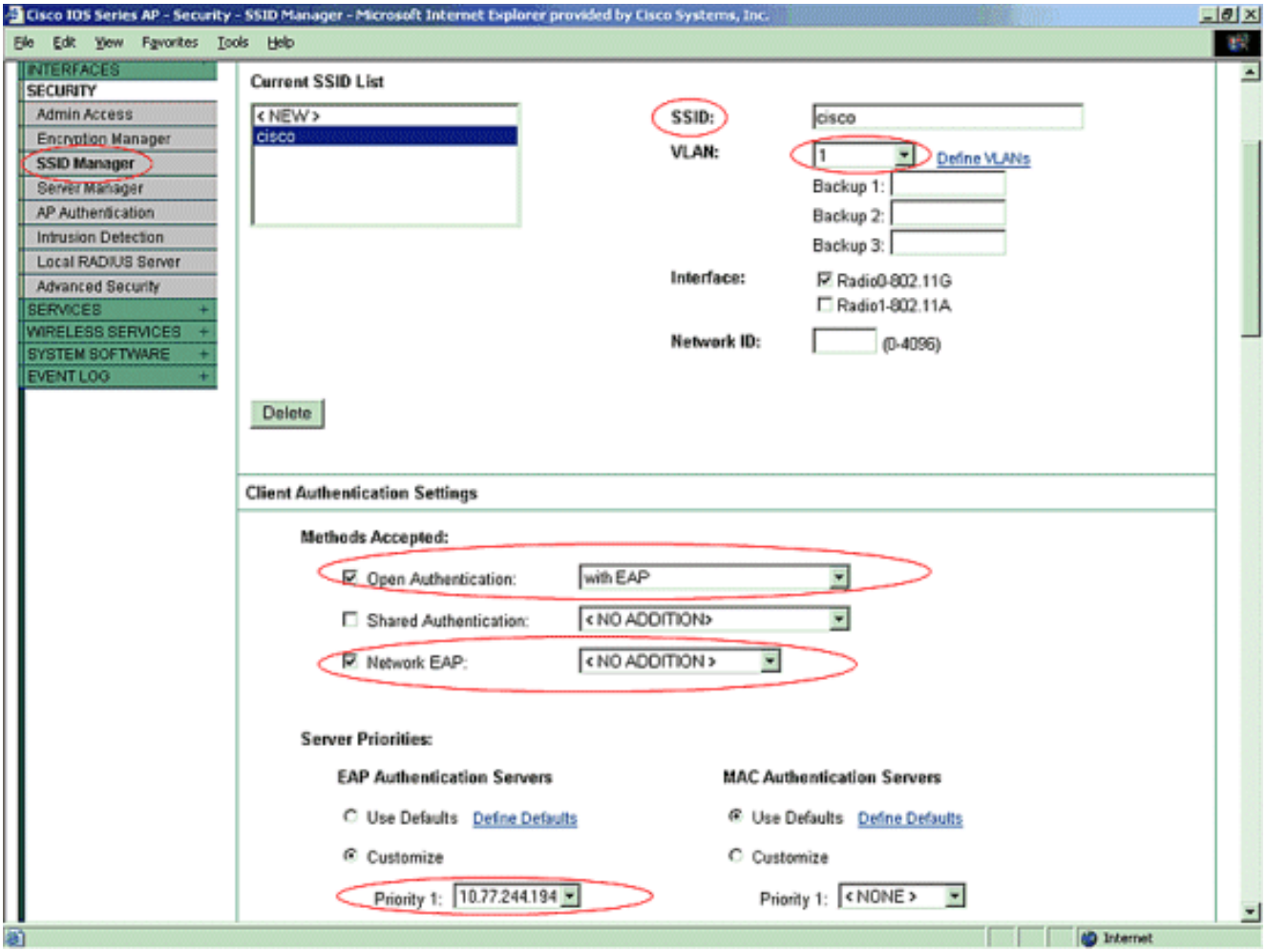
1. 從左側選單中，選擇「安全」選單下的「伺服器管理器」頁籤。配置伺服器並提及此接入點的IP地址，在本例中為10.77.244.194。提及本地Radius伺服器監聽的埠號1812和1813。如圖所示，指定要與本地RADIUS伺服器一起使用的共用金鑰。



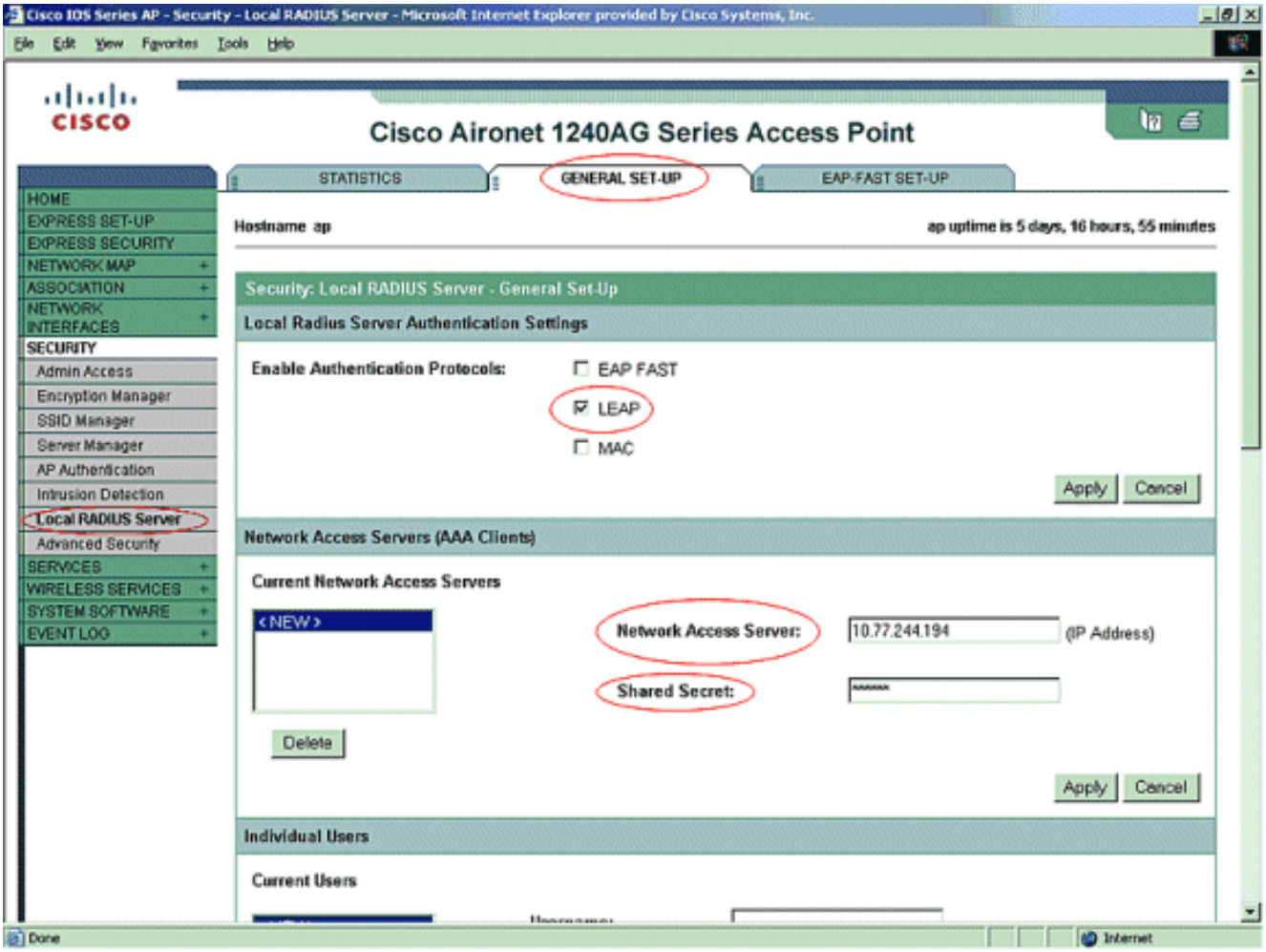
2. 從左側選單中，按一下「安全」選單下的「加密管理器」頁籤。指定要應用的VLAN。指定要使用WEP加密。指定其使用為MANDATORY。使用26位十六進位制字元初始化任何WEP金鑰。此金鑰用於加密廣播和組播資料包。此步驟是可選的。將金鑰大小設定為128位。您還可以選擇40位。在這種情況下，上一步中的WEP金鑰大小必須是10位十六進位制字元。此步驟是可選的。您還可以啟用廣播金鑰輪替，並指定更改廣播金鑰的時間。如果禁用，廣播金鑰仍會使用，但不會更改。此步驟是可選的。**附註：** 對使用LEAP身份驗證的每個VLAN重複執行這些步驟按一下「Apply」。



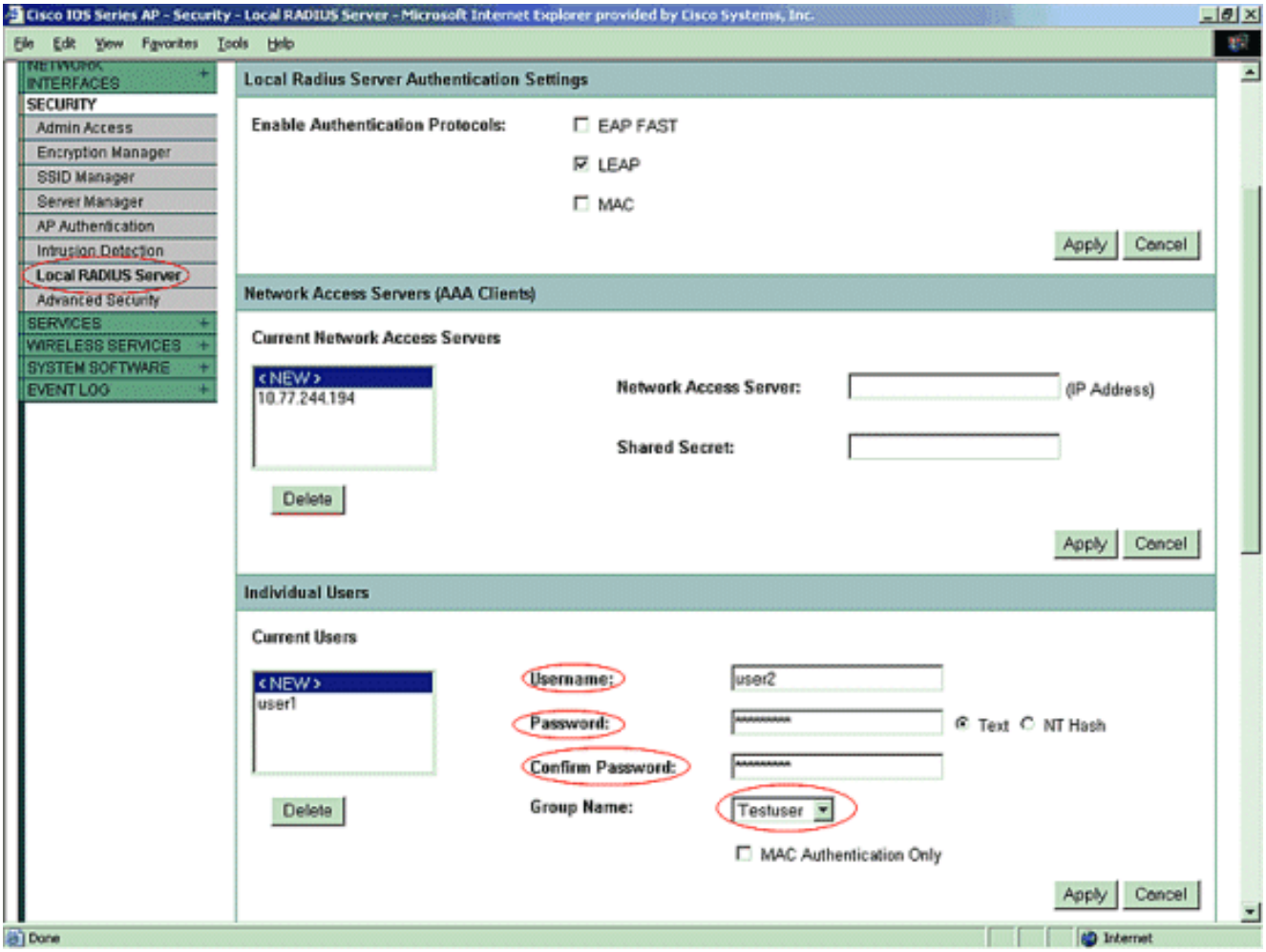
3. 在「Security Menu（安全選單）」下的「SSID Manager（SSID管理器）」頁籤中，執行下列操作：**注意：**在確認基本配置工作正常後，可以稍後新增其他功能和金鑰管理。定義新的SSID並將其與VLAN關聯。在本示例中，SSID與VLAN 1關聯。選中**Open Authentication(With EAP)**。選中**Network EAP(No Addition)**。在**Server Priorities > EAP Authentication Servers**中選擇**Customize**;為**Priority** 1選擇此接入點的**IP地址**。按一下「**Apply**」。



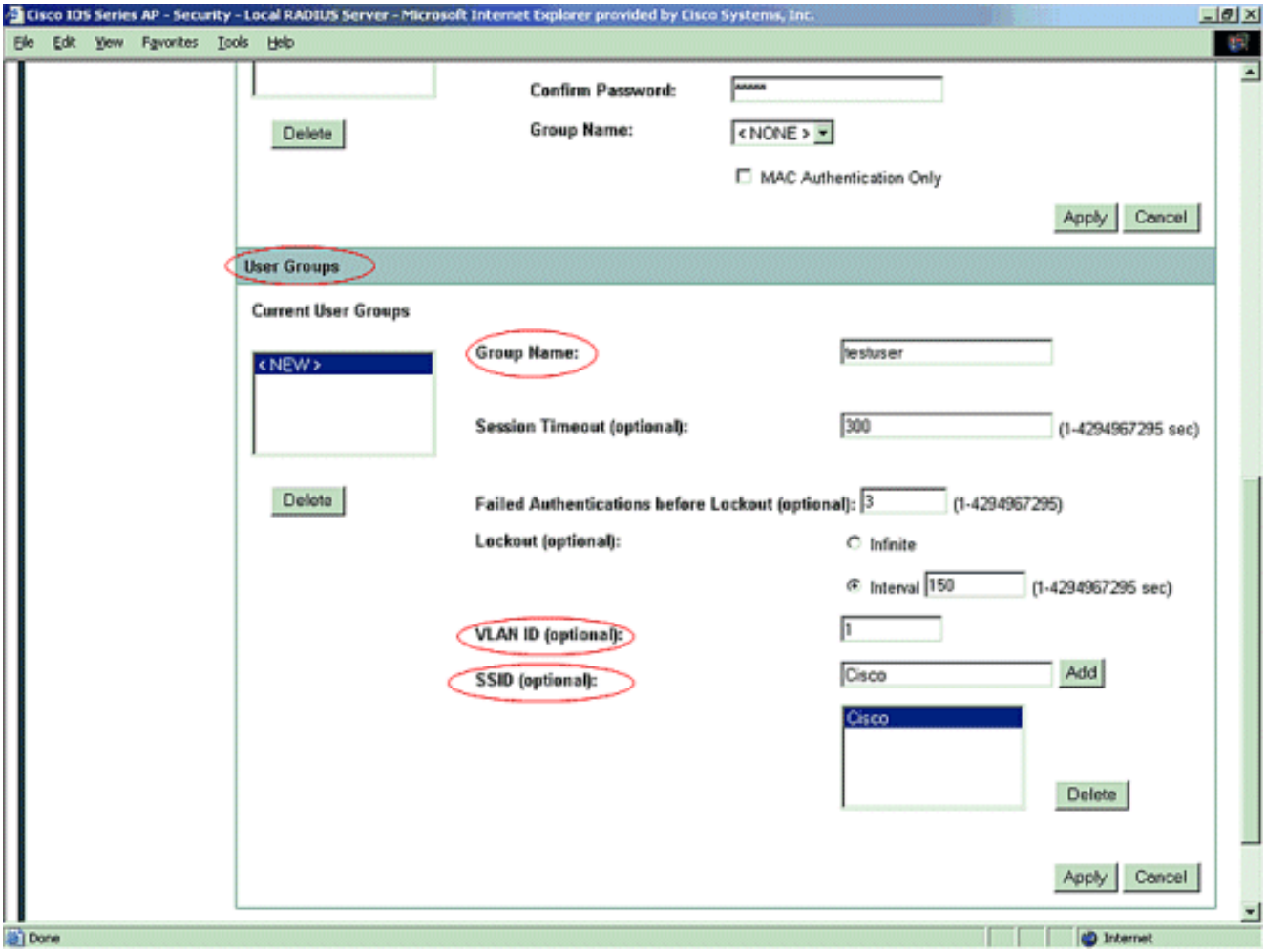
4. 在Security下，按一下General Set-UP頁籤中的Local RADIUS Server在「本地Radius伺服器身份驗證設定」下，選中**LEAP**以確保接受LEAP身份驗證請求。定義RADIUS伺服器的IP地址和共用金鑰。對於本地RADIUS伺服器，這是此AP的IP地址(10.77.244.194)。按一下「**Apply**」。



5. 從General Setup頁籤下的Local RADIUS Server向下滾動，並用其使用者名稱和密碼定義各個使用者。或者，可以將使用者與下一步中定義的組相關聯。這可確保只有特定使用者登入到SSID。**注意**：本地RADIUS資料庫由這些單獨的使用者名稱和密碼組成。



6. 在同一頁上進一步向下滾動，再次從General Set-Up子頁籤下的Local RADIUS Server到User Groups;定義使用者組並將它們與VLAN或SSID關聯。



註：組是可選的。組屬性不會傳遞到Active Directory，並且僅在本地相關。確認基本配置工作正常後，可以稍後新增組。

驗證

使用本節內容，確認您的組態是否正常運作。

- **show radius local-server statistics** — 此命令顯示由本地身份驗證器收集的統計資訊。

```
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** — 此命令顯示接入點上所有已配置RADIUS伺服器組的清單。

疑難排解

疑難排解程序

本節提供與此組態相關的疑難排解資訊。

1. 為了消除阻止身份驗證成功的RF問題的可能性，請將SSID上的方法設定為**Open**，以暫時禁用身份驗證。在GUI — 在SSID Manager頁面上，取消選中**Network-EAP**並選中**Open**。在命令列中 — 使用**authentication open**和**no authentication network-eap eap_methods**命令。如果客戶端成功關聯，則RF不會導致關聯問題。
2. 驗證所有共用金鑰密碼是否已同步。`radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>`和`nas x.x.x.x key <shared_secret>`行必須包含相同的共用金鑰密碼。
3. 刪除有關使用者組的任何使用者組和配置。有時，接入點定義的使用者組和域上的使用者組之間可能會發生衝突。

疑難排解指令

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug dot11 aaa authenticator all** — 此調試顯示客戶端在通過802.1x或EAP進程進行關聯和身份驗證時從身份驗證器（接入點）的角度進行的各種協商。 此偵錯是在Cisco IOS軟體版本12.2(15)JA中匯入。此命令在該版本及更高版本中取代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 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 — 此調試顯示伺服器和客戶端之間的RADIUS協商，在這種情況下，兩者都是接入點。
- debug radius local-server client — 此調試從RADIUS伺服器的角度顯示客戶端的身份驗證。

```
 *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 — 此調試從RADIUS伺服器的角度顯示所有由完成的進程。

相關資訊

- 將接入點配置為本地身份驗證器
- 配置身份驗證型別
- 設定RADIUS和TACACS+伺服器
- 技術支援與文件 - Cisco Systems