ローカル RADIUSサーバの LEAP 認証

目次

はじめに

この資料は Lightweight Extensible Authentication Protocol （ LEAP ）認証に無線クライアントを機能する、提供しましたり、またローカル RADIUSサーバとして機能したものです IOS ® ベースのアクセス ポイントで設定 例を。 これは 12.2(11)JA か以降実行する IOS アクセス ポイントに適当です。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- IOS GUI か CLI の習熟度
- LEAP 認証の後ろの概念の習熟度

コンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Aironet 1240AG シリーズ アクセス アクセス・ポイント
- Cisco IOS ソフトウェア リリース 12.3(8)JA2
- Aironet デスクトップ ユーティリティ 3.6.0.122 を実行する Cisco Aironet 802.11 a/b/g/ワイ

ヤレスアダプタ
- ネットワークの 1 VLAN だけの想定

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ローカル RADIUSサーバ 機能の概要

通常外部 RADIUSサーバがユーザを認証するのに使用されています。 場合によっては、これが適切なソリューションではないことがあります。 この場合、アクセス ポイントは RADIUSサーバとして機能するために作ることができます。 ここでは、ユーザはアクセス ポイントで設定されるローカル データベースに対して認証されます。 これをローカル RADIUS サーバ機能と呼びます。 またローカル RADIUSサーバがアクセス ポイントで特色にするネットワーク使用中の他のアクセス ポイントをすることができます。 これに関する詳細については、他のアクセス ポイントのローカル オーセンティケータを使用するために設定を参照して下さい。

設定

設定はアクセス ポイントの LEAP およびローカル RADIUSサーバ 機能を設定する方法を記述します。 ローカル RADIUSサーバ 機能は Cisco IOS ソフトウェア リリース 12.2(11)JA で導入されました。 外部 RADIUSサーバで LEAP を設定する方法のバックグラウンド情報に関しては RADIUSサーバとの LEAP 認証を参照して下さい。

ほとんどのパスワードベース 認証アルゴリズムと同様に、Cisco LEAP は辞書不正侵入に脆弱です。 これは Cisco LEAP の新しい不正侵入または新しい脆弱性ではないです。 辞書不正侵入を軽減するために強力なパスワード ポリシーを作成して下さいそれは強力なパスワードを含み、新しいパスワードに度々行きます。 辞書不正侵入に関する詳細については辞書不正侵入 LEAP をそれらを防ぐ方法を on Cisco 参照すれば。

この資料は CLI および GUI 両方のためのこの設定を想定します:

1. アクセス ポイントの IP アドレスは **10.77.244.194** です。
2. 使用される SSID は **VLAN 1.**にマップされる **cisco** です。
3. ユーザー名はグループ **Testuser** にマップされる **user2** です、および **user1**。

CLI 設定

アクセス ポイント

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
```

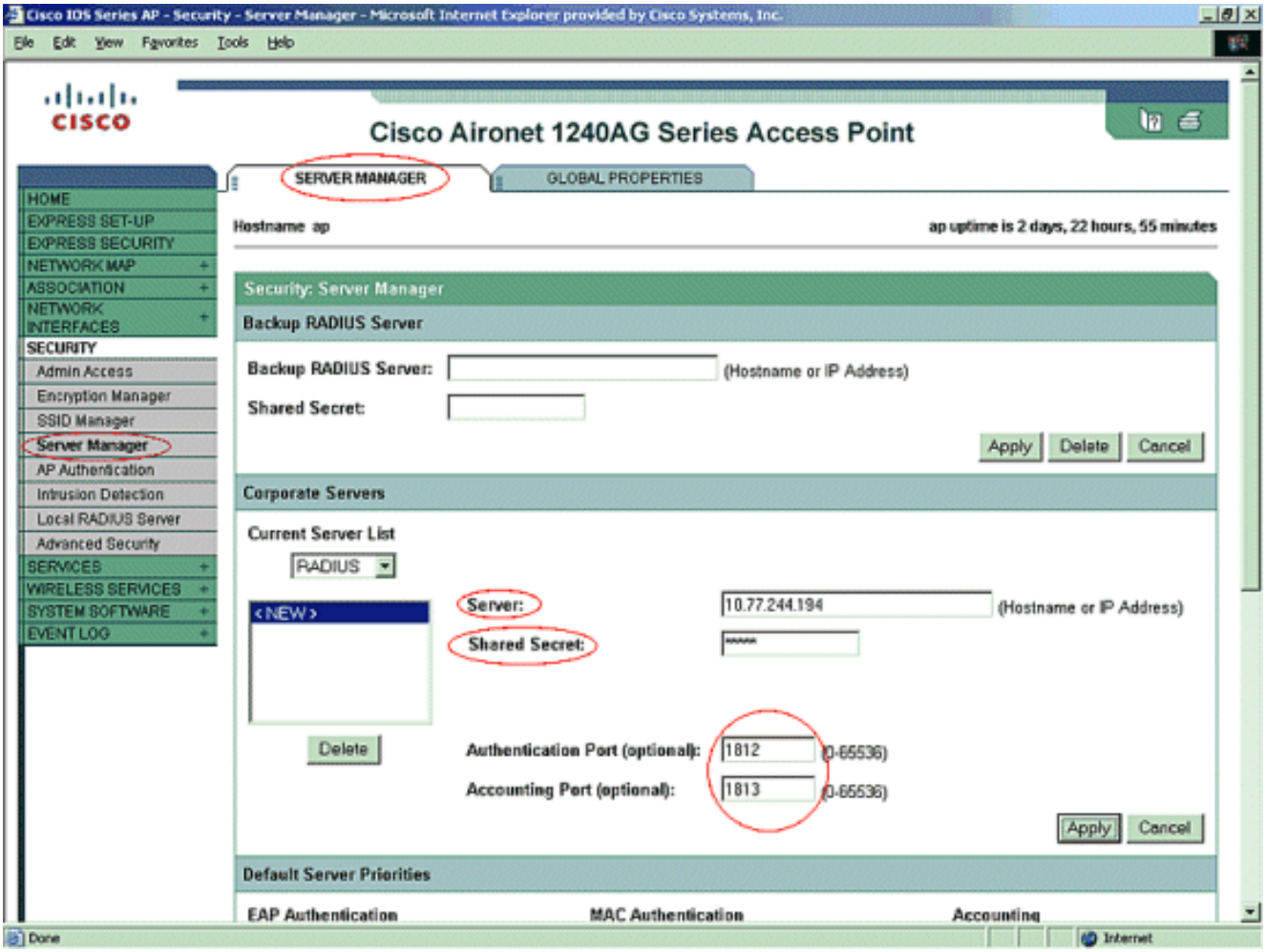
```
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.77.244.194 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.77.244.194 on
ports 1812 and 1813. . . . aaa authentication 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 設定

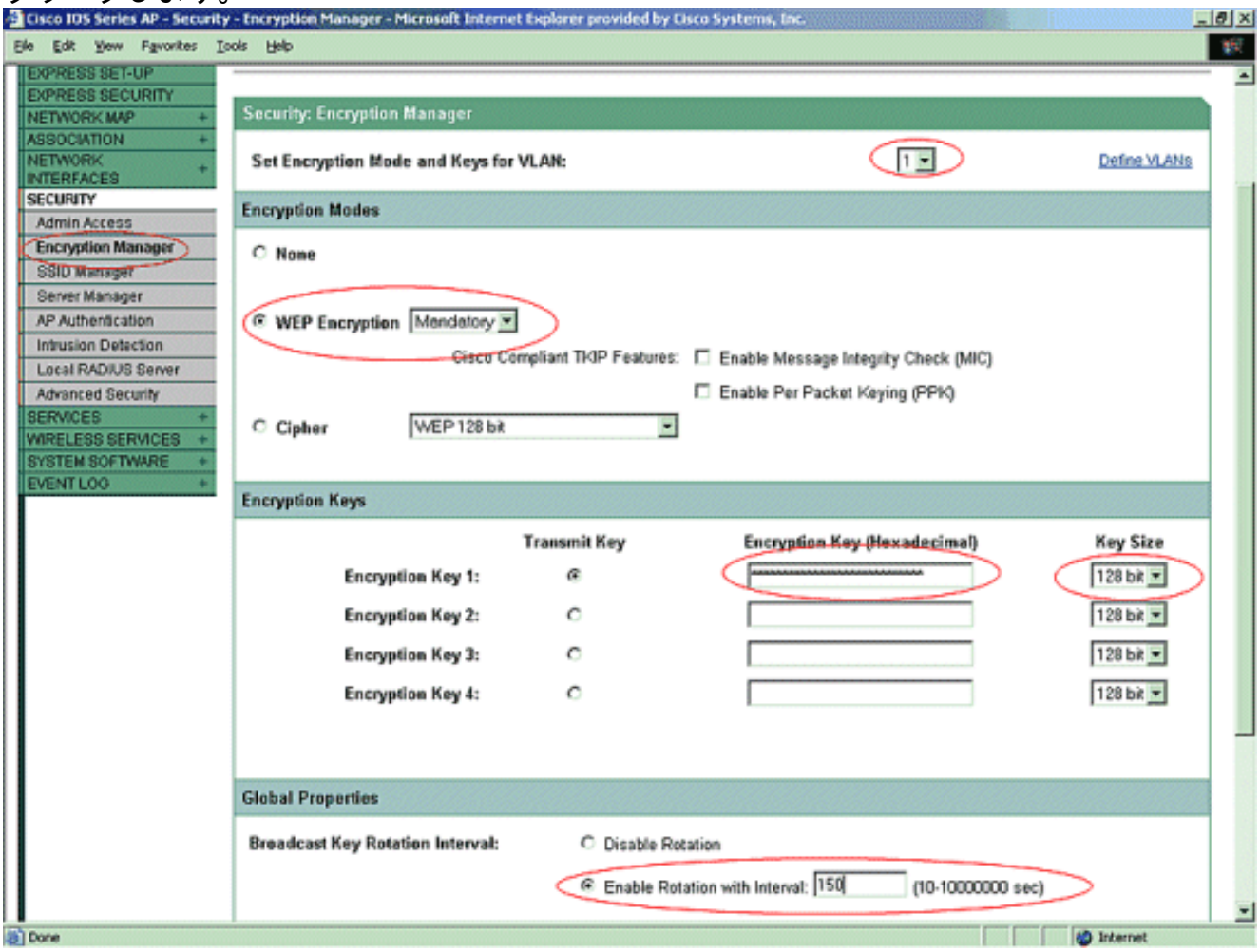
GUI でローカル RADIUSサーバ 機能を設定するためにこれらのステップを完了して下さい:

1. 左側のメニューから、Security メニューの下で Server Manager タブを選択して下さい。サーバを設定し、この例の 10.77.244.194 であるこのアクセス ポイントの IP アドレスを述べて下さい。第 1812 およびローカル RADIUSサーバが受信する 1813 を述べて下さい。図に示すようにローカル RADIUSサーバと使用されるべき共用シークレットを規定 して下さい。

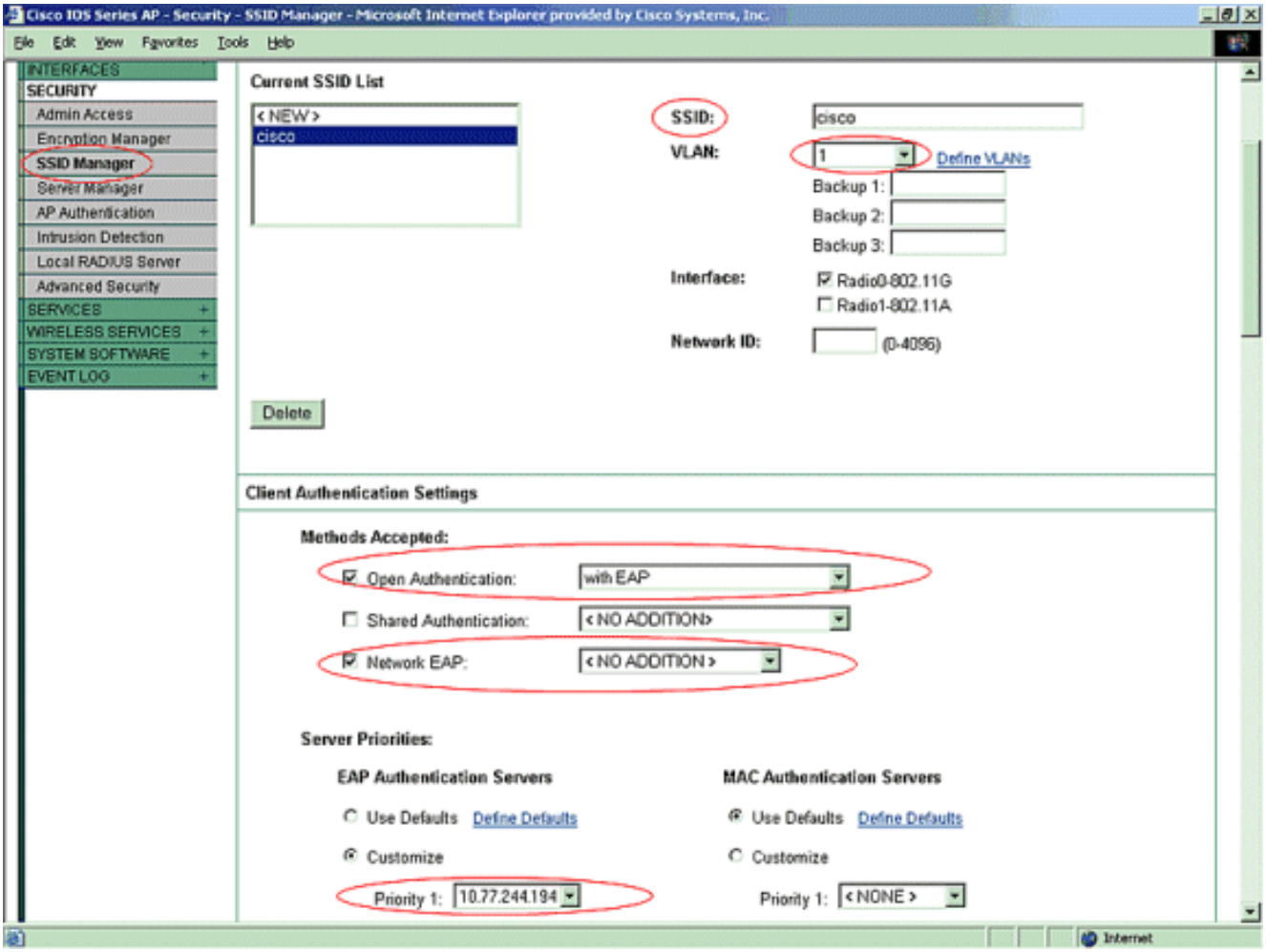


2. 左側のメニューから、Security メニューの下で Encryption Manager タブをクリックして下さい。適用されるべき VLAN を規定 して下さい。WEP暗号化が使用されるべきであること規定 して下さい。使用が MANDATORY であること規定 して下さい。26 ディジット 16 進法文字が付いている WEPキーを初期化して下さい。 このキーがブロードキャストおよびマルチキャスト パケットを暗号化するのに使用されています。 この手順はオプションです。128 ビットにキー サイズを設定 して下さい。 また 40 ビットを選択できます。 この場合、前の手順の WEPキー サイズは 10 ディジット 16 進法文字である必要があります。 この手順はオプションです。またブロードキャスト キー ローテーションを有効に し、時間を規定できますそのあとでブロードキャスト キーは変更されます。 それが無効に なる場合、ブロードキャスト キーはまだ使用されますが、変更されません。 この手順はオプションです。
注: これらのステップは LEAP 認証を使用する各 VLAN のために繰り返されます[Apply] を

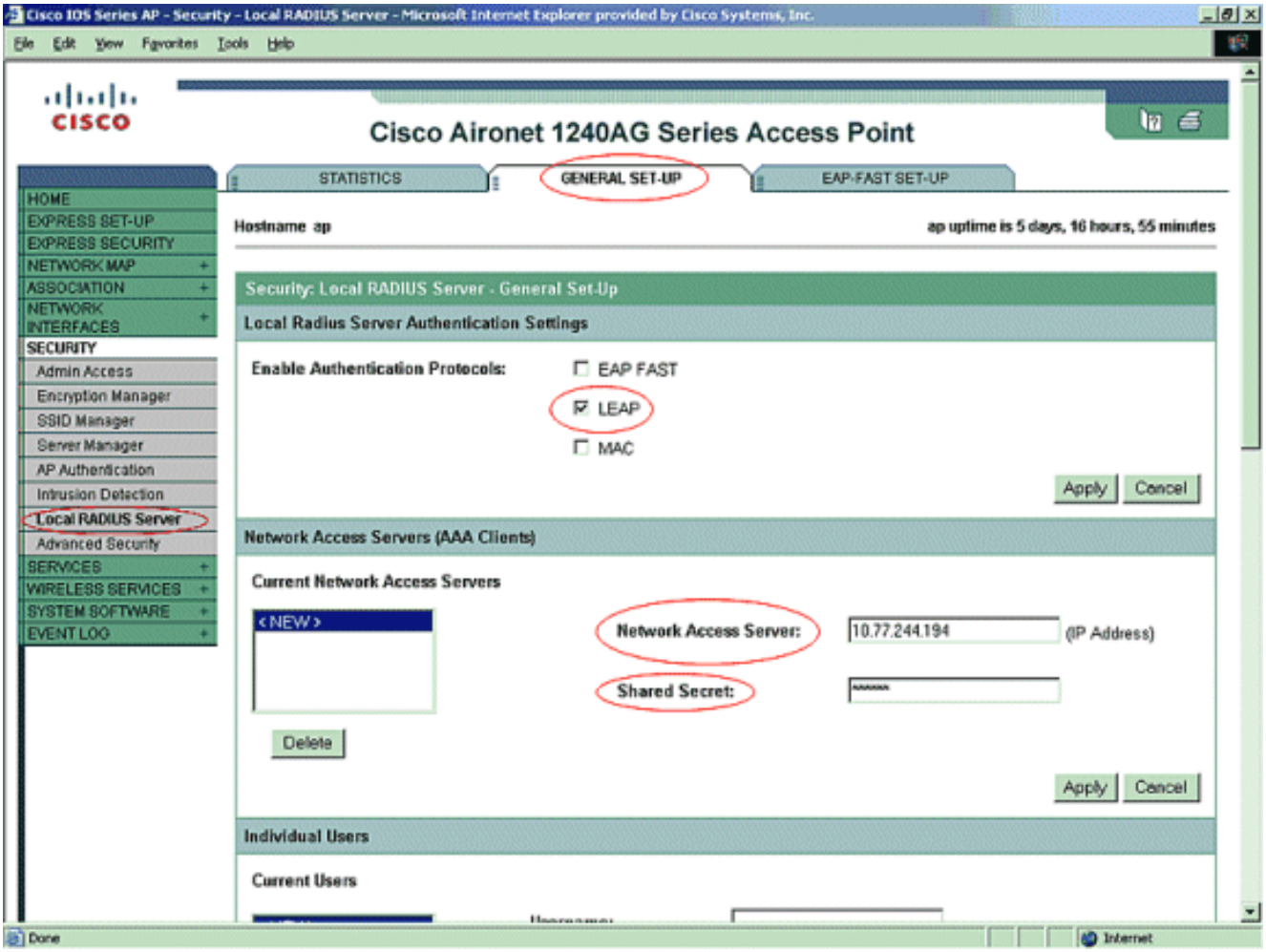
クリックします。



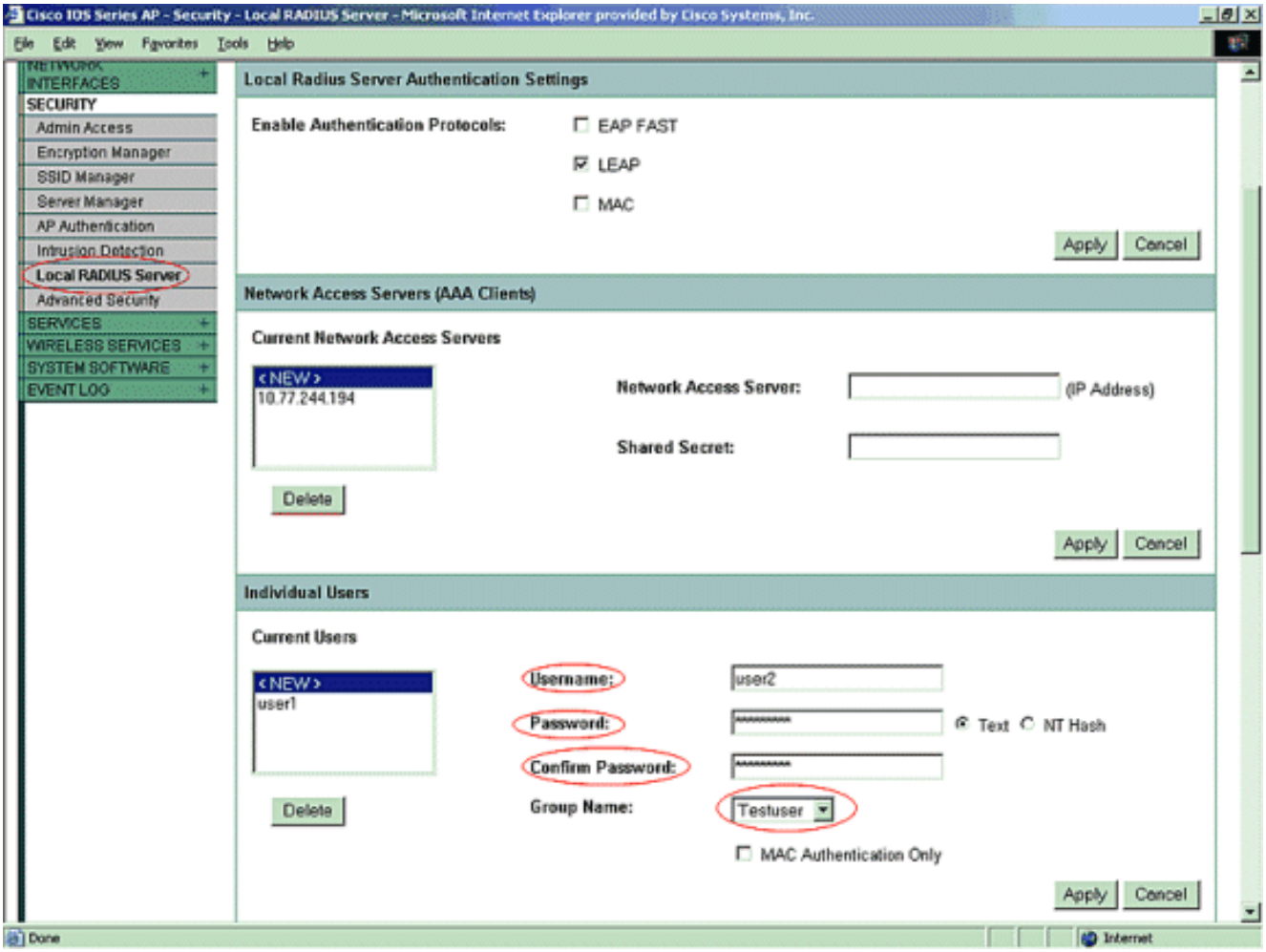
3. Security メニューの下で、SSID Manager タブから、これらのアクションを行って下さい:**注**: 基礎設定は正しく機能することを確認すれば追加機能およびキー管理以降を追加できます。新しい SSID を定義し、VLAN と関連付けて下さい。 この例では、SSID は VLAN 1.と関連付けられます。**開いた認証を**チェックして下さい（**EAP と**）。**ネットワーク EAP（付加無し）を**チェックして下さい。**サーバ 優先順位 > EAP 認証サーバ**から、『Customize』 を選択 して下さい; このアクセス ポイント forPriority **1.**の IP アドレスを選択して下さい。[Apply] をクリックします。



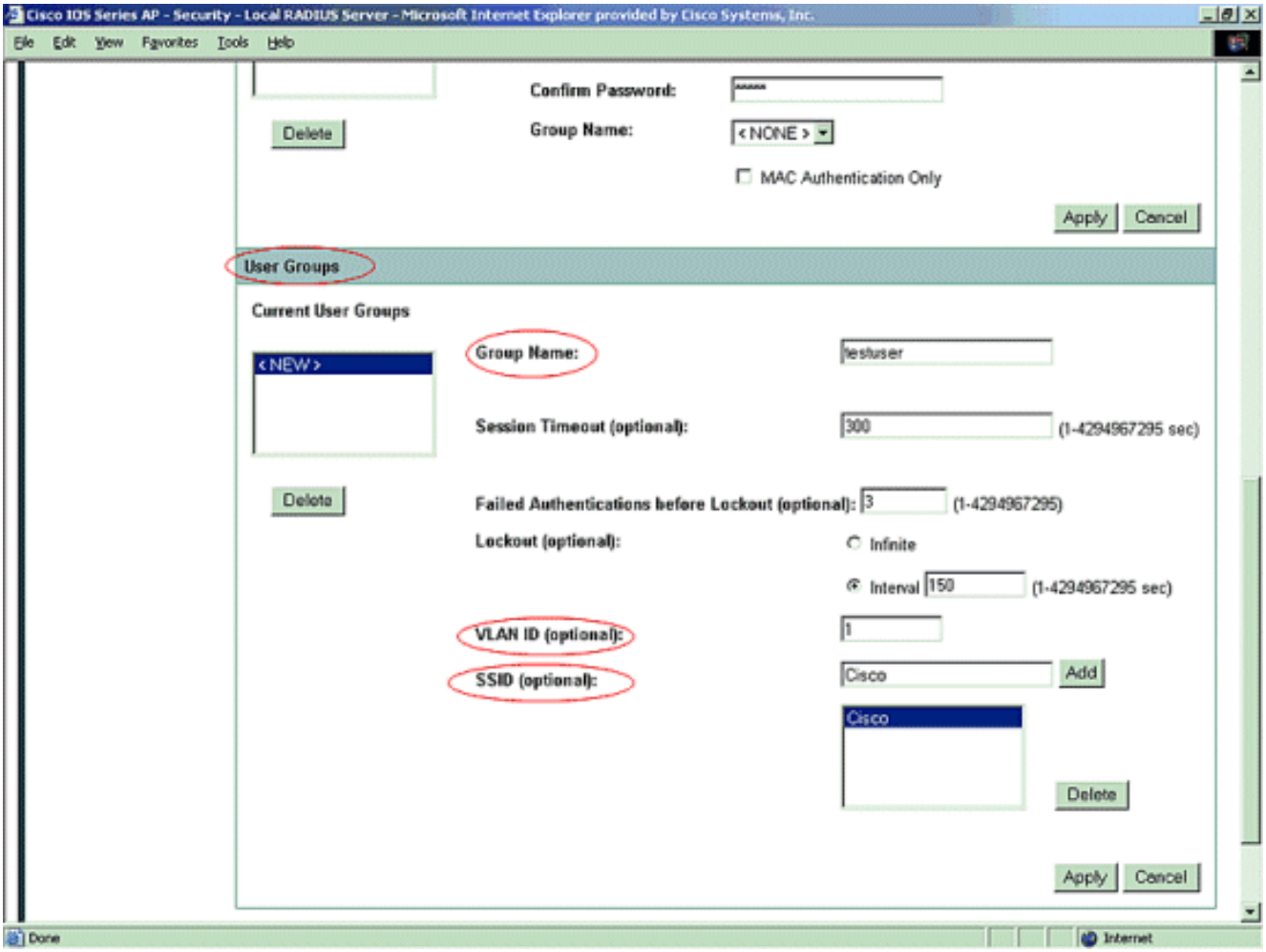
4. セキュリティの下で、General Set-up タブからのローカル RADIUSサーバをクリックして下さいローカル RADIUSサーバ認証設定の下、LEAP Authentication 要求が受け入れられることを確かめるチェック **LEAP**。RADIUSサーバの IP アドレスおよび共用シークレットを定義して下さい。 ローカル RADIUSサーバに関しては、これはこの AP の IP アドレスです（10.77.244.194）。[Apply] をクリックします。



5. ローカル RADIUSサーバから一般の Setup タブの下でスクロールし、ユーザ名 および パスワードの個々のユーザを定義して下さい。 任意で、ユーザはグループに関連付けることができます次のステップで定義される。 これは一定のユーザだけ SSID に記録 することを確かめます。**注:** ローカル RADIUS データベースはこれらの個々のユーザ名 および パスワードで構成されます。



6. 一般の設定 sub タブの下でローカル RADIUSサーバからのユーザグループに同じページで、再度更にスクロールして下さい; ユーザグループを定義し、VLAN か SSID にそれらを関連付けて下さい。



注: グループはオプションです。 グループ属性は Active Directory に通じないし、ローカルでだけ関連しています。 基礎設定は正しく機能することを確認すればグループ以降を追加できます。

確認

ここでは、設定が正常に動作していることを確認します。

- **show radius local-server statistics** —このコマンドはローカル オーセンティケータによって収集される統計情報を表示したものです。

```
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/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
```

- **全半径がサーバグループ**このコマンド アクセス ポイントのすべての設定された RADIUS サーバグループのリストを表示することを**示して下さい。**

トラブルシューティング

トラブルシューティング手順

このセクションでは、この設定に関連するトラブルシューティング情報を提供します。

1. 認証の成功を防ぐ RF 問題の可能性を軽減するために一時的に認証を無効に するために**開くように** SSID の方式を設定 して下さい。GUI から— SSID マネージャ ページで、**ネットワーク EAP の**チェックを外し、**開いた**チェックして下さい。コマンド· ラインから—**開いた**コマンド**認証**および**認証ネットワーク EAP eap_methods を**使用しないで下さい。クライアントが関連付けに成功する場合には、RF はアソシエーションの問題に関係しません。
2. すべての共有秘密パスワードが同期されていることを確認します。 行 `radius x.x.x.x auth-port X acct-port X <shared_secret>` NAS `x.x.x.x <shared_secret>` 同じ共用秘密パスワードが。
3. ユーザグループについてのユーザグループおよび設定を取除いて下さい。 時々競合はアクセス ポイント定義されるユーザグループとドメインのユーザグループの間に発生する場合があります。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **全デバッグ dot11 AAA オーセンティケータは**このデバッグ クライアントがクライアント関連として行き、802.1X か EAP プロセスによってオーセンティケータ (アクセス ポイント) の観点から認証を受けることをさまざまなネゴシエーションに示します。 このデバッグは Cisco IOS ソフトウェア リリース 12.2(15)JA で導入されました。 このコマンドはそれおよび以降のリリースの debug dot11 aaa dot1x all を廃止 します。

```
 *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 —このデバッグはサーバ間の RADIUS ネゴシエーションを示し、この場合、アクセス ポイントであるクライアント。
- debug radius local-server client：この debug コマンドを実行すると、クライアントの認証が RADIUS サーバ側からの視点で表示されます。

```
 *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** —このデバッグは RADIUSサーバによっておよびの観点から実行されるすべてのプロセスを表示します。

関連情報

- ローカル オーセンティケータでアクセス ポイントを設定すること
- 設定
- RADIUS サーバと TACACS+ サーバの設定
- テクニカル サポートとドキュメント – Cisco Systems