Authentification LEAP sur un serveur RADIUS local

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour l'authentification de Lightweight Extensible Authentication Protocol (LEAP) sur un Point d'accès basé sur ® IOS, qui sert les clients sans fil, aussi bien qu'agit en tant que serveur local de RADIUS. Ce s'applique à un Point d'accès IOS qui exécute 12.2(11)JA ou plus tard.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance du GUI ou de CLI IOS
- Connaissance des concepts derrière l'authentification de LEAP

Composants

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Point d'accès de gamme de Cisco Aironet 1240AG

- Version du logiciel Cisco IOS 12.3(8)JA2
- Adaptateur Sans fil du 802.11 a/b/g/de Cisco Aironet qui exécute Aironet Desktop Utility 3.6.0.122
- Acceptation de seulement un VLAN dans le réseau

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Aperçu de caractéristique de serveur de RADIUS de gens du pays

Habituellement un serveur RADIUS externe est utilisé pour authentifier des utilisateurs. Dans certains cas, ce n'est pas une solution faisable. Dans ces situations, un Point d'accès peut être fait pour agir en tant que serveur de RADIUS. Ici, des utilisateurs sont authentifiés contre la base de données locale configurée au Point d'accès. Ceci s'appelle une caractéristique locale de serveur de RADIUS. Vous pouvez également faire d'autres Points d'accès dans l'utilisation de réseau que le serveur local de RADIUS comportent sur un Point d'accès. Pour plus d'informations sur ceci, référez-vous à configurer d'autres Points d'accès pour utiliser l'authentificateur local.

Configurer

La configuration décrit comment configurer la caractéristique de serveur de Radius de LEAP et de gens du pays sur un Point d'accès. La caractéristique locale de serveur de RADIUS a été introduite dans le Logiciel Cisco IOS version 12.2(11)JA. Référez-vous à l'authentification de LEAP avec le serveur de RADIUS pour l'information générale sur la façon dont configurer le LEAP avec un serveur RADIUS externe.

Comme avec la plupart des algorithmes basés sur une authentification par mot de passe, Cisco LEAP est vulnérable aux attaques de dictionnaire. Ce n'est pas une nouvelle attaque ou une nouvelle vulnérabilité de Cisco LEAP. Vous devez créer une stratégie de mot de passe fort pour atténuer des attaques par dictionnaire, cela inclurait des mots de passe fort et fréquenterait de nouveaux mots de passe. Référez-vous à l'attaque par dictionnaire sur le LEAP de Cisco pour plus d'informations sur des attaques par dictionnaire et comment les empêcher.

Ce document suppose cette configuration pour le CLI et le GUI :

1. L'adresse IP du Point d'accès est **10.77.244.194**.
2. Le SSID utilisé est **Cisco**, qui est tracé au **VLAN 1.**
3. Les noms d'utilisateur sont **user1** et **user2**, qui sont tracés au groupe **Testuser**.

Configuration CLI

Point d'accès

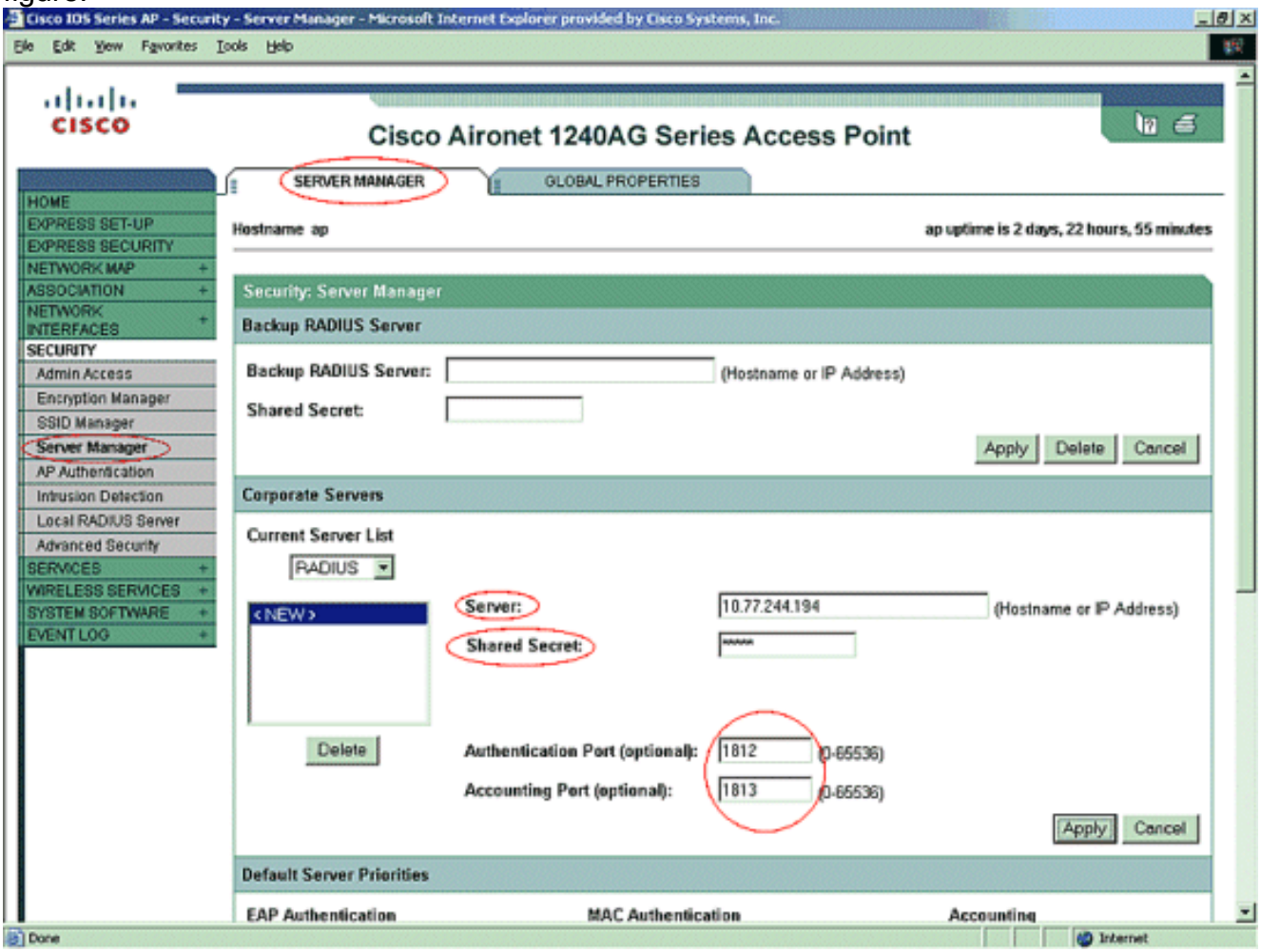
```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.77.244.194 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"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
```

Configuration de la GUI

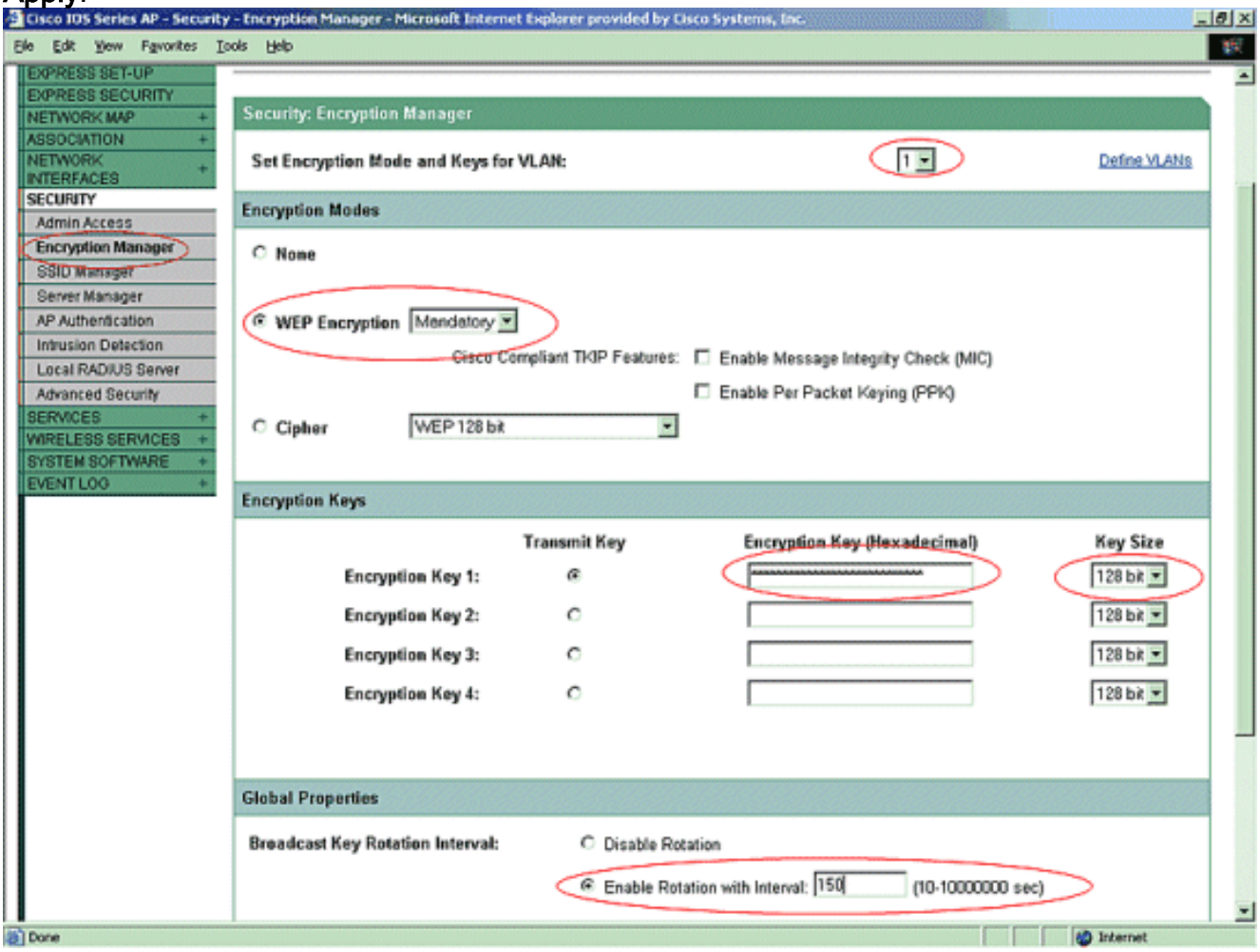
Terminez-vous ces étapes afin de configurer la caractéristique locale de serveur de RADIUS avec le GUI :

1. Du menu dans le côté gauche, choisissez l'onglet de gestionnaire du serveur sous le menu Security.Configurez le serveur et mentionnez l'adresse IP de ce Point d'accès, qui est 10.77.244.194 dans cet exemple.Mentionnez les numéros de port 1812 et 1813 sur lesquels le serveur local de Radius écoute.Spécifiez le secret partagé à utiliser avec le serveur local de RADIUS suivant les indications de la figure.

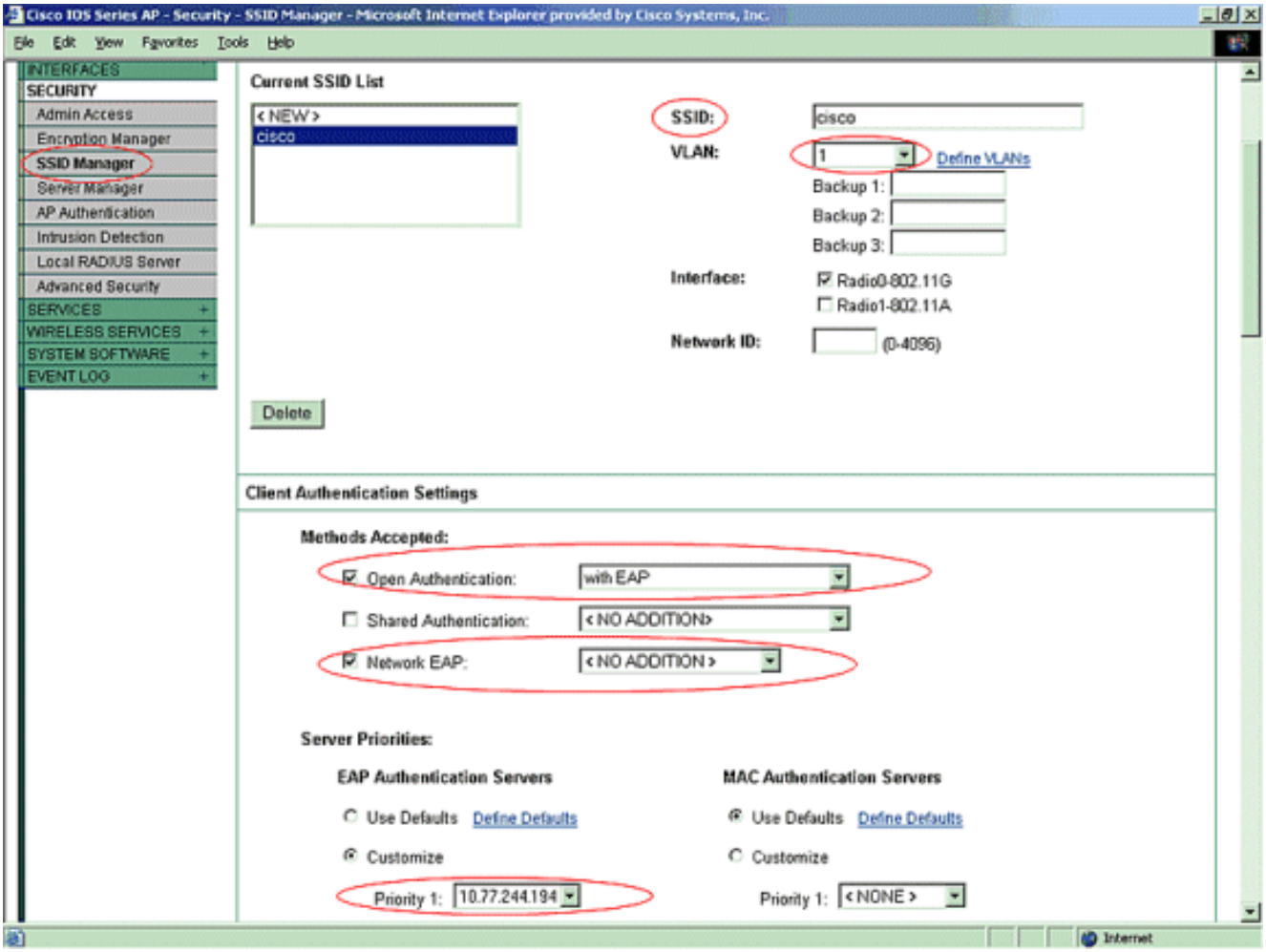


2. Du menu dans le côté gauche, cliquez sur l'onglet de gestionnaire de cryptage sous le menu Security.Spécifiez le VLAN à appliquer.Spécifiez que le cryptage WEP doit être

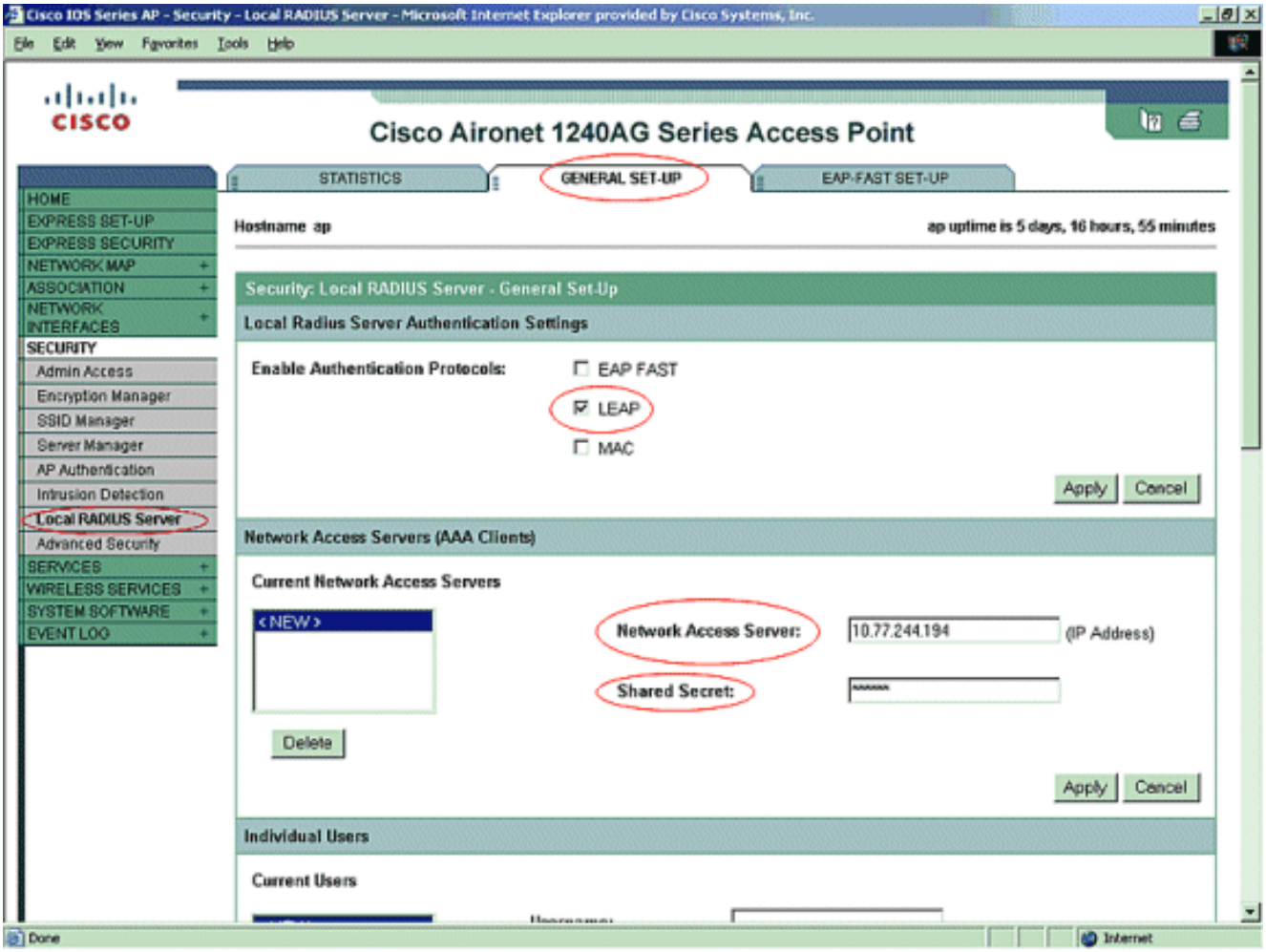
utilisé.Spécifiez que son utilisation est OBLIGATOIRE.Initialisez n'importe quelle clé WEP avec un caractère hexadécimal 26-digit. Cette clé est utilisée pour chiffrer l'émission et les paquets de multidiffusion. Cette étape est facultative.Fixez la taille de clé à 128 bits. Vous pouvez également choisir 40 bits. Dans ce cas, la taille de clé WEP dans l'étape précédente doit être un caractère hexadécimal 10-digit. Cette étape est facultative.Vous pouvez également activer la rotation principale d'émission et spécifier le temps après quoi la clé d'émission est changée. S'il est désactivé, la clé d'émission est toujours utilisée mais pas changée. Cette étape est facultative.**Remarque:** Ces étapes sont répétées pour chaque VLAN qui utilise l'authentification de LEAPCliquez sur
Apply.



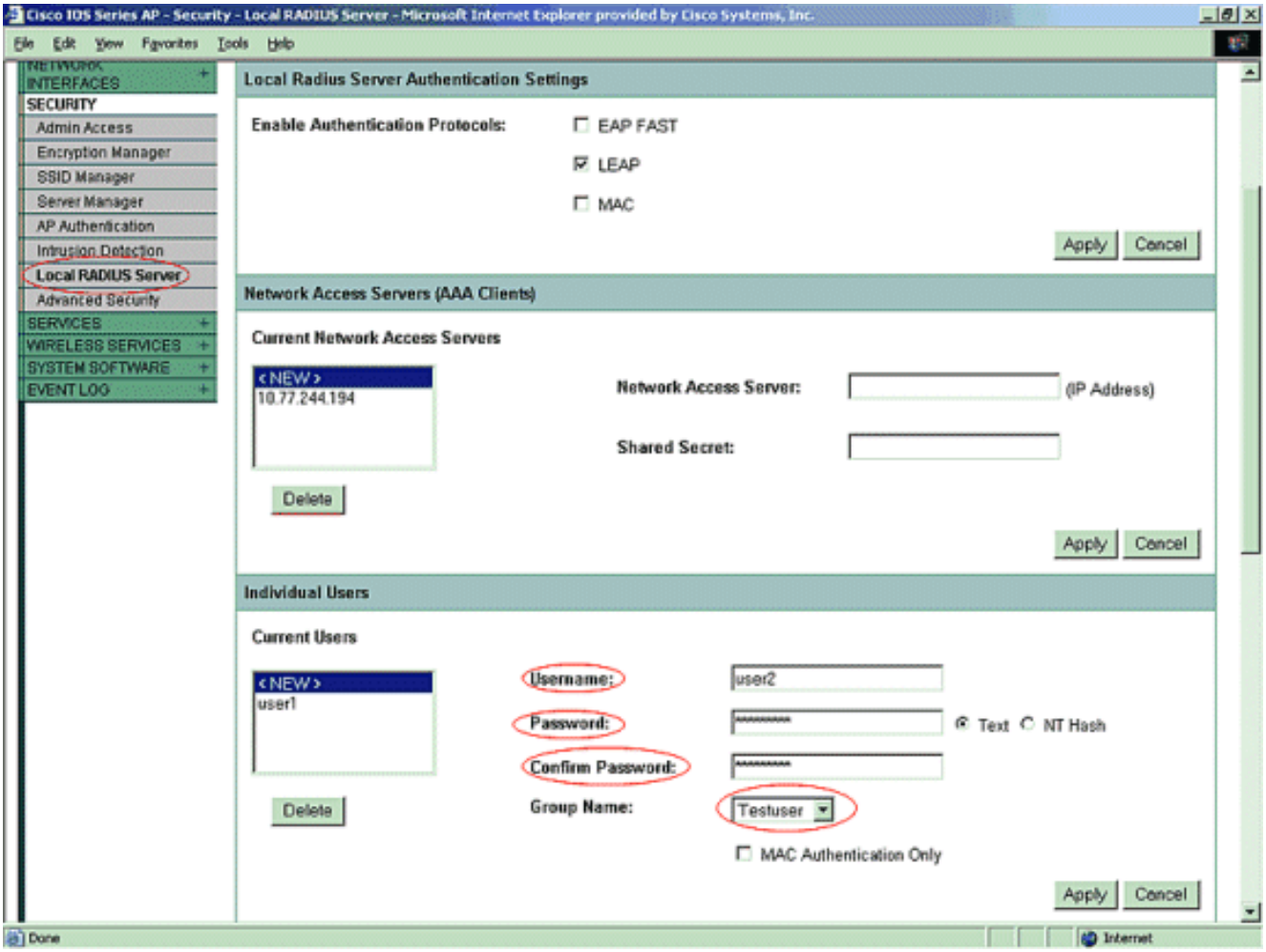
3. Sous le menu Security, de l'onglet de gestionnaire SSID, exécutez ces actions :**Remarque:** Vous pouvez ajouter les fonctionnalités supplémentaires et la gestion des clés plus tard, une fois que vous confirmez que la configuration de base fonctionne correctement.Définissez un nouveau SSID et associez-le avec un VLAN. Dans cet exemple, le SSID est associé avec le VLAN 1.**Authentification ouverte de** contrôle **(With EAP).EAP de réseau de** contrôle **(aucun ajout).Des serveurs prioritaires > d'authentification EAP de serveur**, choisissez **personnalisent** ; choisissez l'adresse IP de ce forPriority **1. de** Point d'accès.Cliquez sur
Apply.



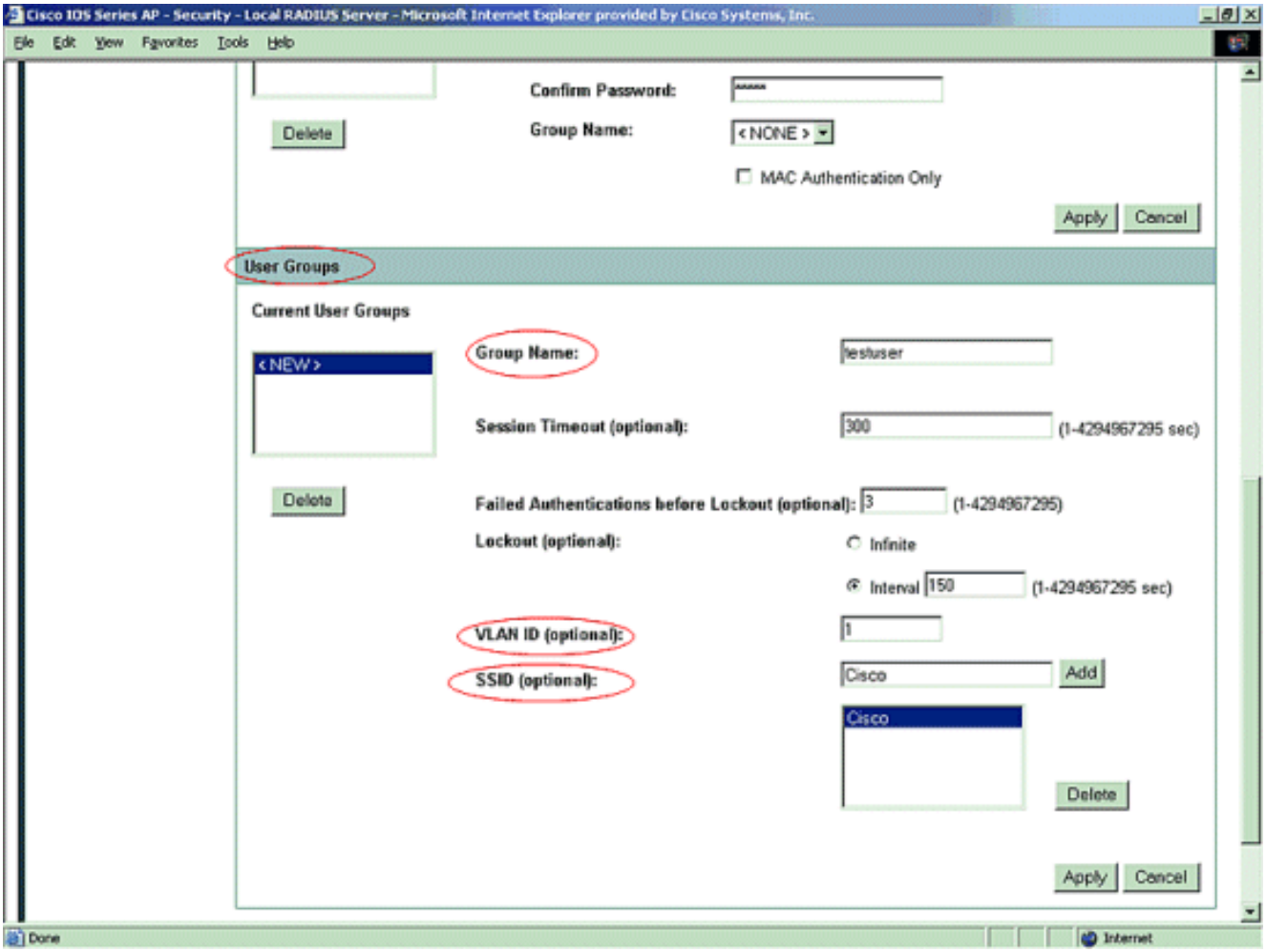
4. Sous la Sécurité, serveur de RADIUS de gens du pays de clic de l'onglet de configuration généraleSous des configurations d'authentification de serveur de Radius de gens du pays, **LEAP de** contrôle pour s'assurer que des demandes d'authentification de LEAP sont reçues.Définissez l'adresse IP et le secret partagé du serveur de RADIUS. Pour le serveur de RADIUS de gens du pays, c'est l'adresse IP de cet AP (10.77.244.194).Cliquez sur **Apply**.



5. Faites descendre l'écran du serveur de RADIUS de gens du pays sous l'onglet de configuration générale et définissez les utilisateurs individuels avec leurs noms d'utilisateur et mot de passe. Sur option, des utilisateurs peuvent être associés aux groupes, qui est défini dans l'étape suivante. Ceci veille ce seulement certain log d'utilisateurs dans un SSID.**Remarque:** La base de données locale de RADIUS est composée de ces différents noms d'utilisateur et mot de
passe.



6. Faites défiler plus loin vers le bas à la même page, de nouveau du serveur local de RADIUS sous l'onglet de sous-titre de configuration générale aux groupes d'utilisateurs ; définissez les groupes d'utilisateurs et associez-les à un VLAN ou à un SSID.



Remarque: Les groupes sont facultatifs. Les attributs de groupe ne passent pas au Répertoire actif et sont seulement localement appropriés. Vous pouvez ajouter des groupes plus tard, une fois que vous confirmez que la configuration de base fonctionne correctement.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- **show radius local-server statistics** — Cette commande affiche des statistiques collectées par l'authentificateur local.

```
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
```

- **le show radius server-group entièrement** cette commande affiche une liste de tous les servers-group configurés de RADIUS sur le Point d'accès.

Dépanner

Procédure de dépannage

Cette section fournit l'information de dépannage concernant cette configuration.

1. Afin d'éliminer la possibilité de questions rf empêchant l'authentification réussie, placez la méthode sur le SSID **pour s'ouvrir** pour désactiver temporairement l'authentification.Du GUI — À la page de gestionnaire SSID, décochez le **Network-EAP** et vérifiez **ouvert**.De la ligne de commande — N'utilisez l'**authentication open de** commandes et **aucun eap_methods d'authentication network-eap**.Si le client s'associe avec succès, le rf ne contribue pas au problème d'association.
2. Vérifiez que tous les mots de passe secret partagés sont synchronisés. Les lignes `<shared_secret> principal du l'acct-port X du l'authentique-port X de l'hôte x.x.x.x de RADIUS-serveur et <shared_secret> de clé du` nas `x.x.x.x doivent contenir la` même chose mot de passe secret partagé.
3. Retirez n'importe quels groupes d'utilisateurs et configuration au sujet des groupes d'utilisateurs. Parfois les conflits peuvent se produire entre les groupes d'utilisateurs définis par le Point d'accès, et les groupes d'utilisateurs sur le domaine.

Dépannage des commandes

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **l'authentificateur de debug dot11 aaa entièrement** ceci mettent au point des expositions les diverses négociations qu'un client intervient pendant que le client s'associe et authentifie par le 802.1x ou le processus d'EAP de la perspective de l'authentificateur (Point d'accès). Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Ce dot1x tout de debug dot11 aaa d'obsoletes de commande dans cela et des versions ultérieures.

```
 *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]
```

- authentification de debug radius — Ceci mettent au point des expositions les négociations de RADIUS entre le serveur et client, qui, dans ce cas, sont le Point d'accès.
- client de debug radius local-server — Ceci mettent au point des expositions l'authentification du client de la perspective du serveur de RADIUS.

```
 *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]
```

- **paquets de debug radius local-server** — Ceci mettent au point des expositions tous les processus faits par et de la perspective du serveur de RADIUS.

Informations connexes

- Configurer un Point d'accès comme authentificateur local
- Configuration des types d'authentification
- Configuration des serveurs RADIUS et TACACS+
- Support et documentation techniques - Cisco Systems