LEAP-Authentifizierung auf einem lokalen RADIUS-Server

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die LEAP-Authentifizierung (Lightweight Extensible Authentication Protocol) auf einem IOS®-basierten Access Point, der für die Wireless-Clients verwendet wird und als lokaler RADIUS-Server fungiert. Dies gilt für einen IOS Access Point, der 12.2(11)JA oder höher ausführt.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Vertrautheit mit der IOS-GUI oder der CLI
- Vertrautheit mit den Konzepten für die LEAP-Authentifizierung

Komponenten

Die Informationen in diesem Dokument basieren auf diesen Software- und Hardwareversionen.

- Cisco Aironet Access Point der Serie 1240AG
- Cisco IOS Softwareversion 12.3(8)JA2
- Cisco Aironet 802.11 a/b/g/Wireless-Adapter mit Aironet Desktop Utility 3.6.0.122
- Annahme von nur einem VLAN im Netzwerk

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Übersicht über die lokale RADIUS-Serverfunktion

In der Regel wird ein externer RADIUS-Server zur Authentifizierung von Benutzern verwendet. In einigen Fällen ist dies keine praktikable Lösung. In diesen Situationen kann ein Access Point als RADIUS-Server fungieren. Hier werden Benutzer anhand der lokalen Datenbank authentifiziert, die im Access Point konfiguriert wurde. Dies wird als Funktion für einen lokalen RADIUS-Server bezeichnet. Sie können auch festlegen, dass die Funktion Lokaler RADIUS-Server eines Access Points für andere Access Points im Netzwerk verwendet wird. Weitere Informationen hierzu finden Sie unter Konfigurieren weiterer Access Points zum Verwenden des lokalen Authentifizierers.

Konfigurieren

Die Konfiguration beschreibt die Konfiguration der LEAP- und Local Radius-Serverfunktion auf einem Access Point. Die Funktion für lokale RADIUS-Server wurde in Version 12.2(11)JA der Cisco IOS-Software eingeführt. Hintergrundinformationen zur Konfiguration von LEAP mit einem externen RADIUS-Server finden Sie unter LEAP-Authentifizierung mit RADIUS-Server.

Wie bei den meisten kennwortbasierten Authentifizierungsalgorithmen ist Cisco LEAP anfällig für Wörterbuchangriffe. Dies ist kein neuer Angriff oder keine neue Schwachstelle von Cisco LEAP. Sie müssen eine strenge Kennwortrichtlinie erstellen, um Wörterbuchangriffe zu verhindern, die sichere Passwörter und häufige neue Passwörter beinhalten. Weitere Informationen zu Wörterbuchangriffen und deren Verhinderung finden Sie unter Dictionary Attack auf Cisco LEAP.

In diesem Dokument wird diese Konfiguration sowohl für die CLI als auch für die GUI vorausgesetzt:

1. Die IP-Adresse des Access Points lautet **10.77.244.194**.
2. Der verwendete SSID ist **cisco**, der **VLAN 1** zugeordnet ist.
3. Die Benutzernamen sind **user1** und **user2**, die der Gruppe **Testuser** zugeordnet sind.

CLI-Konfiguration

Access Point
ap#**show running-config**

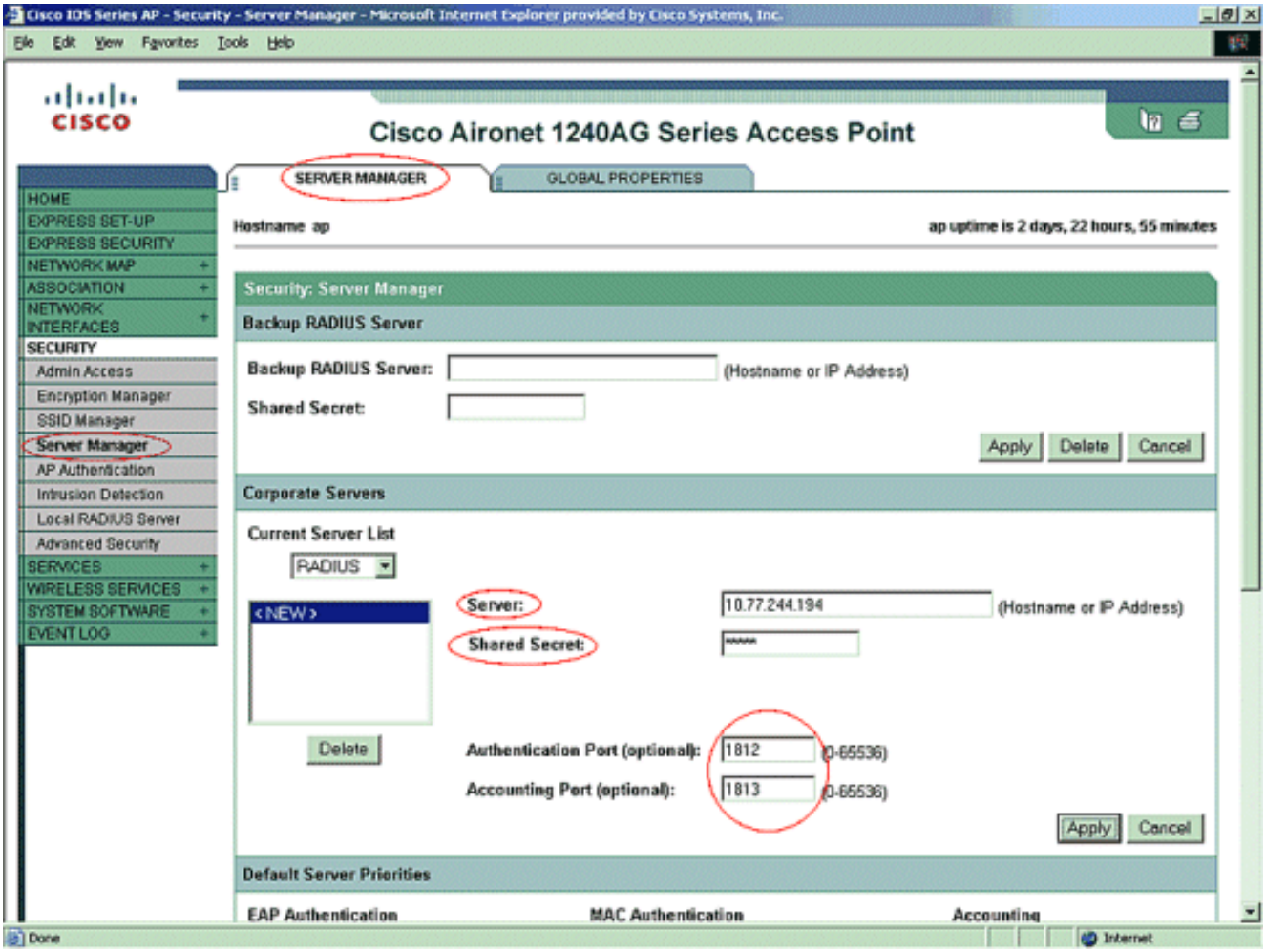
```
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.77.244.194 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that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

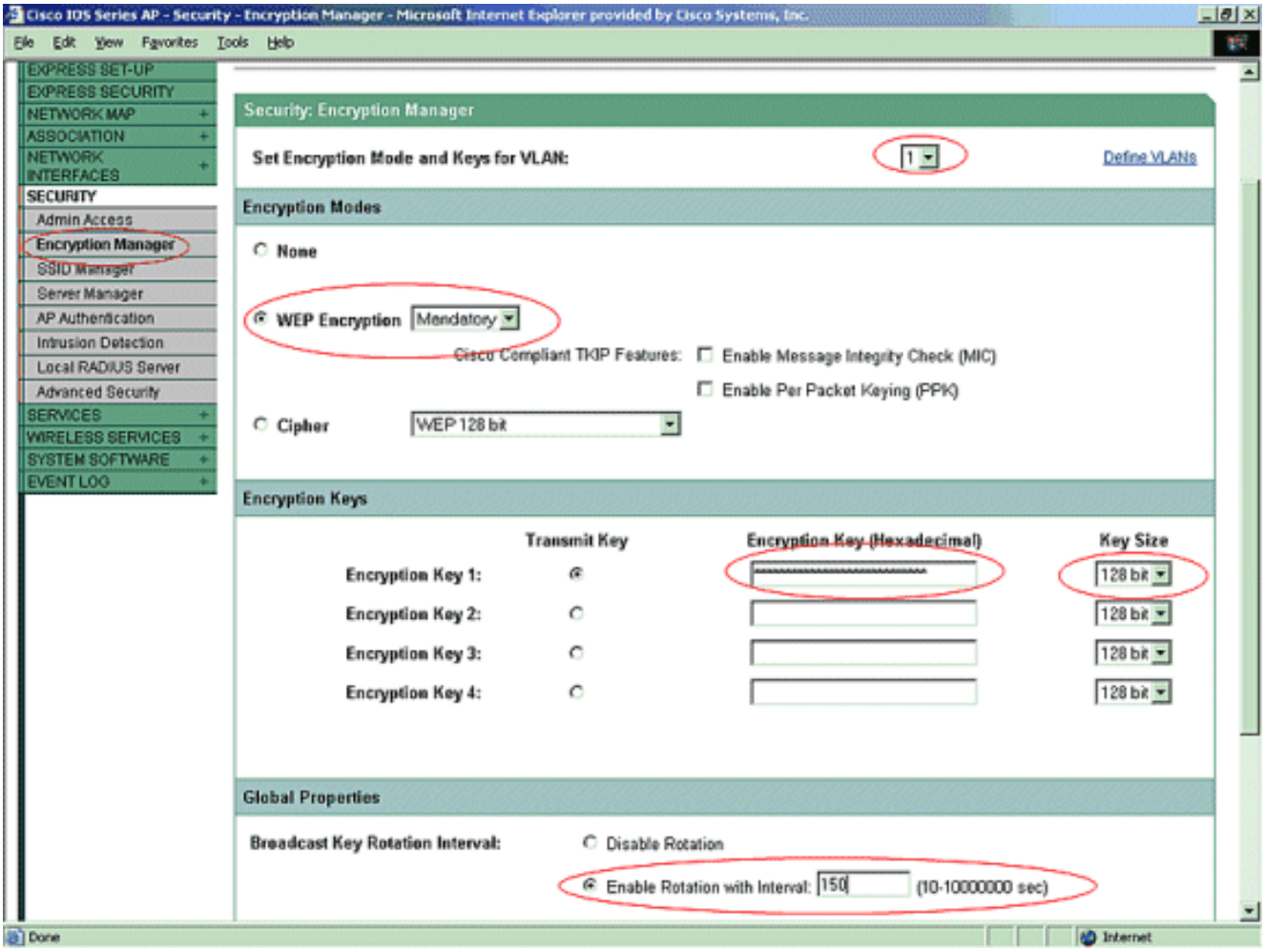
Gehen Sie wie folgt vor, um die Funktion für den lokalen RADIUS-Server über die Benutzeroberfläche zu konfigurieren:

1. Wählen Sie im Menü auf der linken Seite im Menü Sicherheit die Registerkarte Server Manager aus.Konfigurieren Sie den Server, und geben Sie die IP-Adresse dieses Access Points an, die in diesem Beispiel 10.77.244.194 lautet.Nennen Sie die Portnummern 1812 und 1813, auf denen der Local Radius-Server lauscht.Geben Sie den gemeinsam genutzten geheimen Schlüssel für den lokalen RADIUS-Server wie in der Abbildung dargestellt an.

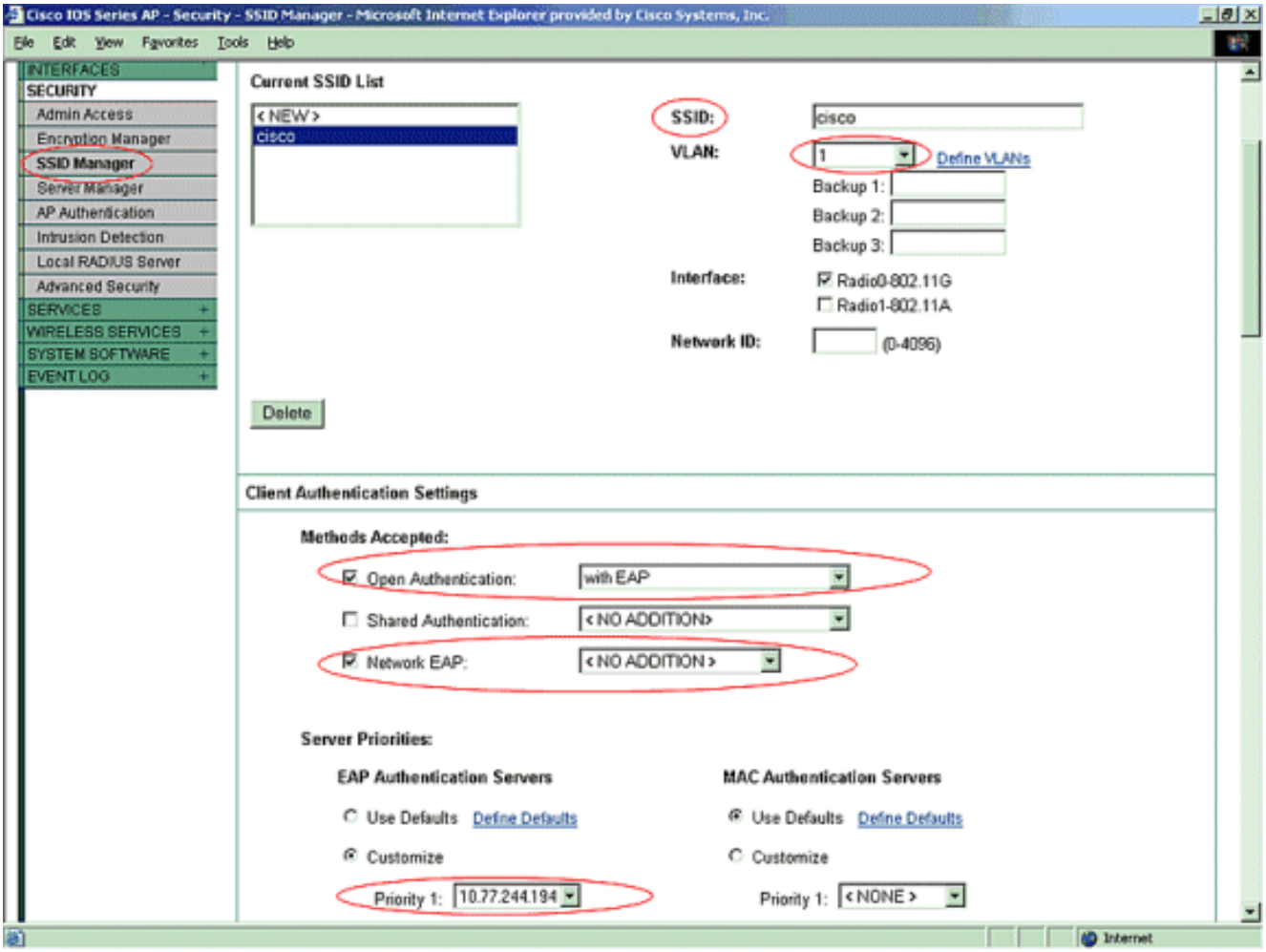


2. Klicken Sie im Menü auf der linken Seite im Menü Sicherheit auf die Registerkarte Verschlüsselungs-Manager.Geben Sie das anzuwendende VLAN an.Geben Sie an, dass die WEP-Verschlüsselung verwendet werden soll.Geben Sie an, dass die Verwendung MANDATORY ist.Initialisieren Sie einen beliebigen WEP-Schlüssel mit einem 26-stelligen Hexadezimalzeichen. Dieser Schlüssel wird zur Verschlüsselung von Broadcast- und

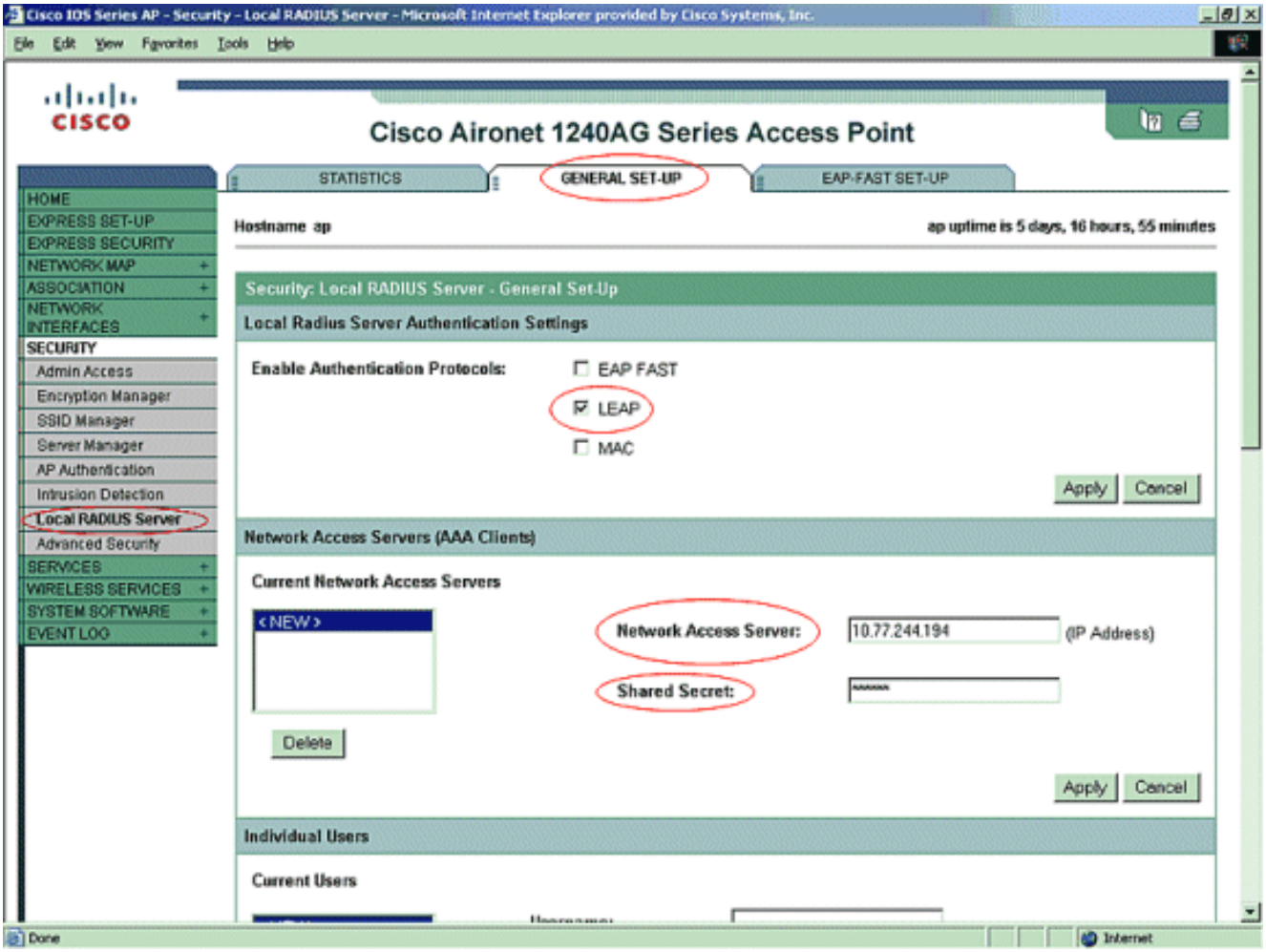
Multicast-Paketen verwendet. Dieser Schritt ist optional.Legen Sie die Schlüssellänge auf 128 Bit fest. Sie können auch 40 Bit auswählen. In diesem Fall muss die WEP-Schlüsselgröße im vorherigen Schritt ein 10-stelliges Hexadezimalzeichen sein. Dieser Schritt ist optional.Sie können auch die Umdrehung des Broadcast-Schlüssels aktivieren und die Zeit angeben, nach der der Broadcast-Schlüssel geändert wird. Wenn sie deaktiviert ist, wird der Broadcast-Schlüssel weiterhin verwendet, aber nicht geändert. Dieser Schritt ist optional.**Hinweis:** Diese Schritte werden für jedes VLAN wiederholt, das die LEAP-Authentifizierung verwendet.Klicken Sie auf **Übernehmen**.



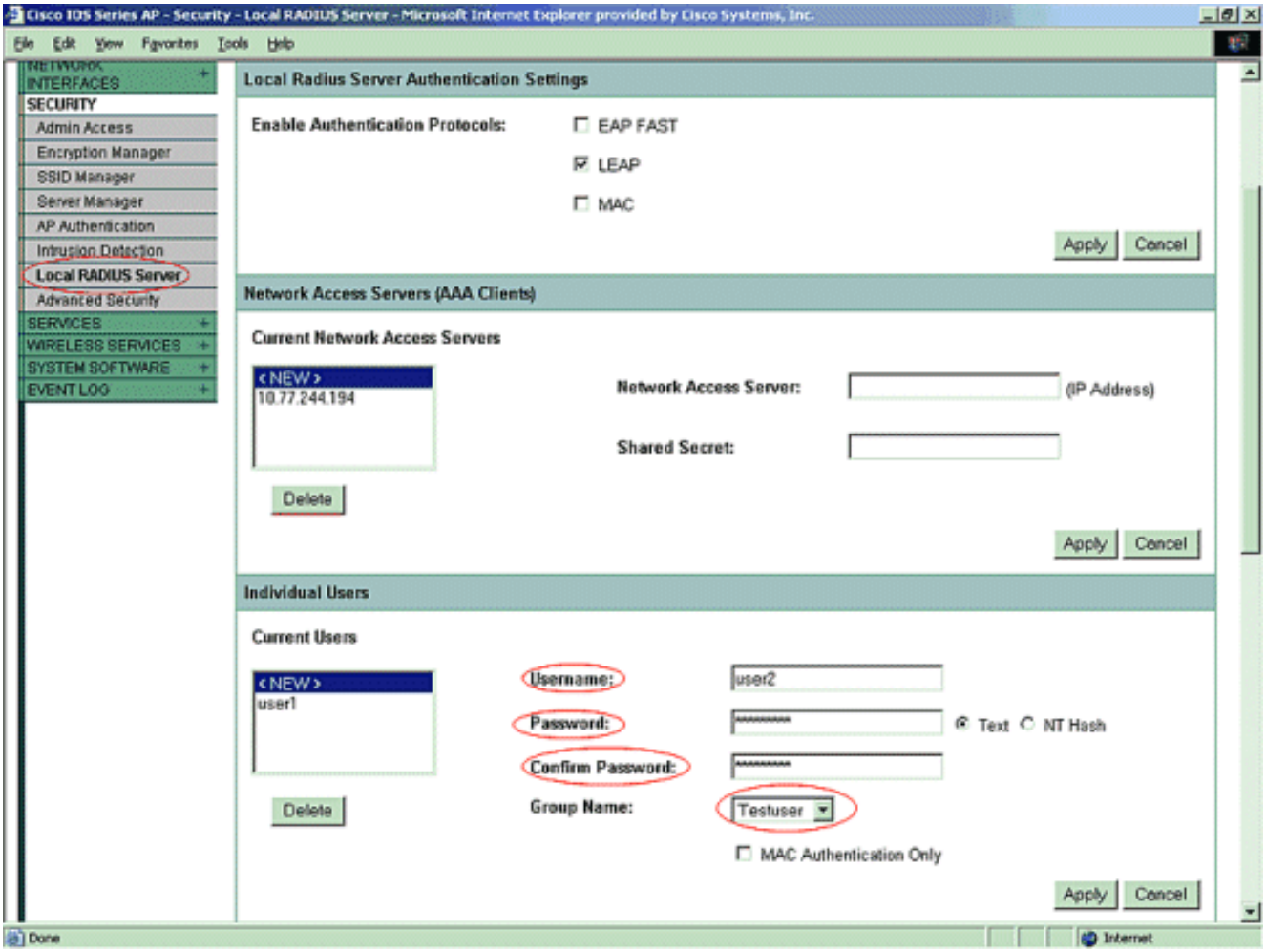
3. Führen Sie im Sicherheitsmenü von der Registerkarte SSID Manager die folgenden Schritte aus:**Hinweis:** Sie können zu einem späteren Zeitpunkt zusätzliche Funktionen und die Schlüsselverwaltung hinzufügen, sobald Sie bestätigen, dass die Basiskonfiguration ordnungsgemäß funktioniert.Definieren Sie eine neue SSID, und ordnen Sie sie einem VLAN zu. In diesem Beispiel ist die SSID VLAN 1 zugeordnet.Aktivieren Sie **Open Authentication (With EAP)**.Aktivieren Sie **Network EAP (No Addition)**.Wählen Sie unter **Serverprioritäten > EAP-Authentifizierungsserver** die Option **Anpassen**. Wählen Sie die IP-Adresse dieses Access Points **fürPriorität 1 aus**.Klicken Sie auf **Übernehmen**.



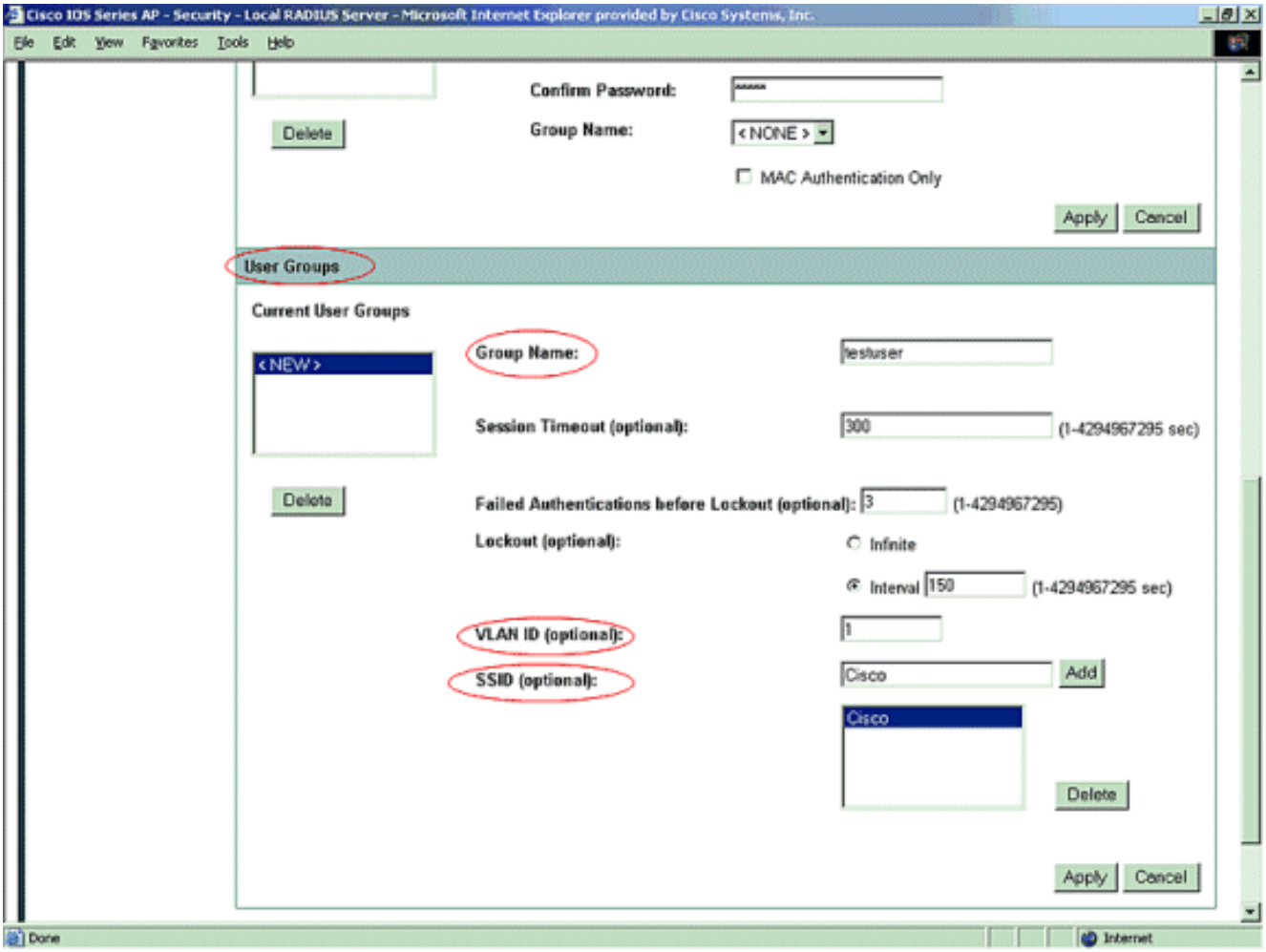
4. Klicken Sie unter "Sicherheit" auf der Registerkarte "Allgemeine Einrichtung" auf Lokaler RADIUS-Server.Aktivieren Sie unter Lokale Radius-Server-Authentifizierungseinstellungen die Option **LEAP**, um sicherzustellen, dass LEAP-Authentifizierungsanforderungen akzeptiert werden.Definieren Sie die IP-Adresse und den gemeinsamen geheimen Schlüssel des RADIUS-Servers. Für den lokalen RADIUS-Server ist dies die IP-Adresse dieses AP (10.77.244.194).Klicken Sie auf **Übernehmen**.



5. Blättern Sie auf der Registerkarte für die allgemeine Einrichtung vom lokalen RADIUS-Server nach unten, und definieren Sie die einzelnen Benutzer mit ihren Benutzernamen und Kennwörtern. Optional können Benutzer Gruppen zugeordnet werden, was im nächsten Schritt definiert wird. Dadurch wird sichergestellt, dass sich nur bestimmte Benutzer bei einer SSID anmelden.**Hinweis:** Die lokale RADIUS-Datenbank besteht aus diesen einzelnen Benutzernamen und
Kennwörtern.



6. Blättern Sie auf derselben Seite weiter nach unten, und wechseln Sie wieder vom lokalen RADIUS-Server unter der Unterregisterkarte "Allgemeine Einrichtung" zu "Benutzergruppen". Benutzergruppen definieren und sie einem VLAN oder einer SSID zuordnen.



Hinweis: Gruppen sind optional. Die Gruppenattribute werden nicht an Active Directory übergeben und sind nur lokal relevant. Sie können später Gruppen hinzufügen, sobald Sie die korrekte Basiskonfiguration bestätigt haben.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- **show radius local-server statistics** - Dieser Befehl zeigt Statistiken an, die vom lokalen Authentifizierer gesammelt wurden.

```
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**: Dieser Befehl zeigt eine Liste aller konfigurierten RADIUS-Servergruppen am Access Point an.

Fehlerbehebung

Fehlerbehebungsverfahren

Dieser Abschnitt enthält Informationen zur Fehlerbehebung, die für diese Konfiguration relevant sind.

1. Um die Möglichkeit von RF-Problemen zu vermeiden, die eine erfolgreiche Authentifizierung verhindern, legen Sie die Methode auf der SSID auf **Öffnen fest**, um die Authentifizierung vorübergehend zu deaktivieren.Aus der GUI - Deaktivieren Sie auf der Seite SSID Manager die Option **Network-EAP** und aktivieren Sie **Open (Öffnen)**.Über die Befehlszeile - Verwenden Sie die Befehle **Authentifizierung offen** und **keine Authentifizierung Netzwerk-eap eap_methods**.Wenn der Client erfolgreich eine Zuordnung vornimmt, trägt RF nicht zum Zuordnungsproblem bei.
2. Überprüfen Sie, ob alle gemeinsam genutzten geheimen Kennwörter synchronisiert sind. Die Zeilen `radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>` und `der Schlüssel nas x.x.x.x <shared_secret>` müssen dasselbe geheime Kennwort enthalten.
3. Entfernen Sie alle Benutzergruppen und die Konfiguration von Benutzergruppen. Manchmal können Konflikte zwischen vom Access Point definierten Benutzergruppen und Benutzergruppen in der Domäne auftreten.

Befehle zur Fehlerbehebung

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug dot11 aaa authentiator all** - Dieses Debuggen zeigt die verschiedenen Verhandlungen, die ein Client durchführt, wenn der Client eine 802.1x- oder EAP-Verbindung herstellt und sich authentifiziert, und zwar aus Sicht des Authentifizierers (Access Point). Diese Fehlerbehebung wurde in Version 12.2(15)JA der Cisco IOS-Software eingeführt. Mit diesem Befehl wird Debug dot11 aaa dot1x in diesen und späteren Versionen ersetzt.

```
 *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 (Debug-Radius-Authentifizierung) - Dieses Debugging zeigt die RADIUS-Verhandlungen zwischen Server und Client, die beide in diesem Fall der Access Point sind.
- debug radius local-server client - Dieses Debuggen zeigt die Authentifizierung des Clients aus Sicht des RADIUS-Servers an.

```
 *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 pakets** - Dieses Debuggen zeigt alle Prozesse an, die vom RADIUS-Server durchgeführt wurden, und aus dessen Sicht.

Zugehörige Informationen

- Konfigurieren eines Access Points als lokaler Authentifizierer

- Konfigurieren von Authentifizierungstypen
- Konfigurieren von RADIUS- und TACACS+-Servern
- Technischer Support und Dokumentation - Cisco Systems