

LEAP-verificatie op een lokale RADIUS-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Componenten](#)

[Conventies](#)

[Overzicht van de functies van lokale RADIUS-servers](#)

[Configureren](#)

[CLI-configuratie](#)

[GUI-configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Procedure voor probleemoplossing](#)

[Opdrachten voor probleemoplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de lichtgewicht uitgebreide verificatie Protocol (LEAP)-verificatie op een op IOS[®] gebaseerd access point, dat de draadloze client dient, evenals een lokale RADIUS-server. Dit is van toepassing op een IOS-access point dat 12.2(11)JA of hoger heeft.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Bekendheid met IOS GUI of CLI
- Bekendheid met de concepten achter de MAP-verificatie

Componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies.

- Cisco Aironet 1240AG Series access point
- Cisco IOS-software release 12.3(8)BY2
- Cisco Aironet 802.11a/b/g/draadloze adapter voor gebruik van Aironet-

desktophulpprogramma 3.6.0.12

- Aanneمة van slechts één VLAN in het netwerk

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\)](#) voor meer informatie over documentconventies.

Overzicht van de functies van lokale RADIUS-servers

Meestal wordt een externe RADIUS-server gebruikt om gebruikers voor authentiek te verklaren. In sommige gevallen is dit geen haalbare oplossing. In deze situaties kan een access point worden gemaakt om als een RADIUS-server te fungeren. Hier worden gebruikers geauthentiseerd tegen de lokale database die in het access point is ingesteld. Dit wordt een lokale RADIUS-serverfunctie genoemd. U kunt ook andere access points in het netwerk gebruiken als de functie Local RADIUS Server op een access point. Raadpleeg voor meer informatie hierover het [configureren](#) van [andere access points om de lokale verificator te gebruiken](#).

Configureren

De configuratie beschrijft hoe u de functies LEAP en Local Radius Server op een toegangspunt kunt configureren. De lokale RADIUS-serverfunctie is geïntroduceerd in Cisco IOS-software-release 12.2(11)JA. Raadpleeg de [LEAP-verificatie met RADIUS-server](#) voor achtergrondinformatie over de manier waarop u LEAP met een externe RADIUS-server kunt configureren.

Net als bij de meeste op een wachtwoord gebaseerde authenticatiealgoritmen, is Cisco LEAP kwetsbaar voor woordenboekaanvallen. Dit is geen nieuwe aanval of nieuwe kwetsbaarheid van Cisco LEAP. U moet een sterk wachtwoordbeleid maken om de gevolgen van de woordenboekaanvallen te verzachten. Dat zou sterke wachtwoorden en frequente nieuwe wachtwoorden omvatten. Raadpleeg de [woordenboekaanval op Cisco LEAP](#) voor meer informatie over woordenboekaanvallen en de manier waarop u deze kunt voorkomen.

Dit document is alleen beschikbaar in combinatie met de CLI- en GUI-indeling:

1. Het IP-adres van het access point is **10.77.24.194**.
2. SSID gebruikt is **cisco**, dat aan **VLAN 1** in kaart wordt gebracht.
3. De gebruikersnamen zijn **user1** en **user2**, die in kaart zijn gebracht door de groep **Testuser**.

CLI-configuratie

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 nhash password1 group
testuser !--- Individual user user user2 nhash
password2 group testuser !--- Individual user !--- These
individual users comprise the Local Database ! radius-

```

```

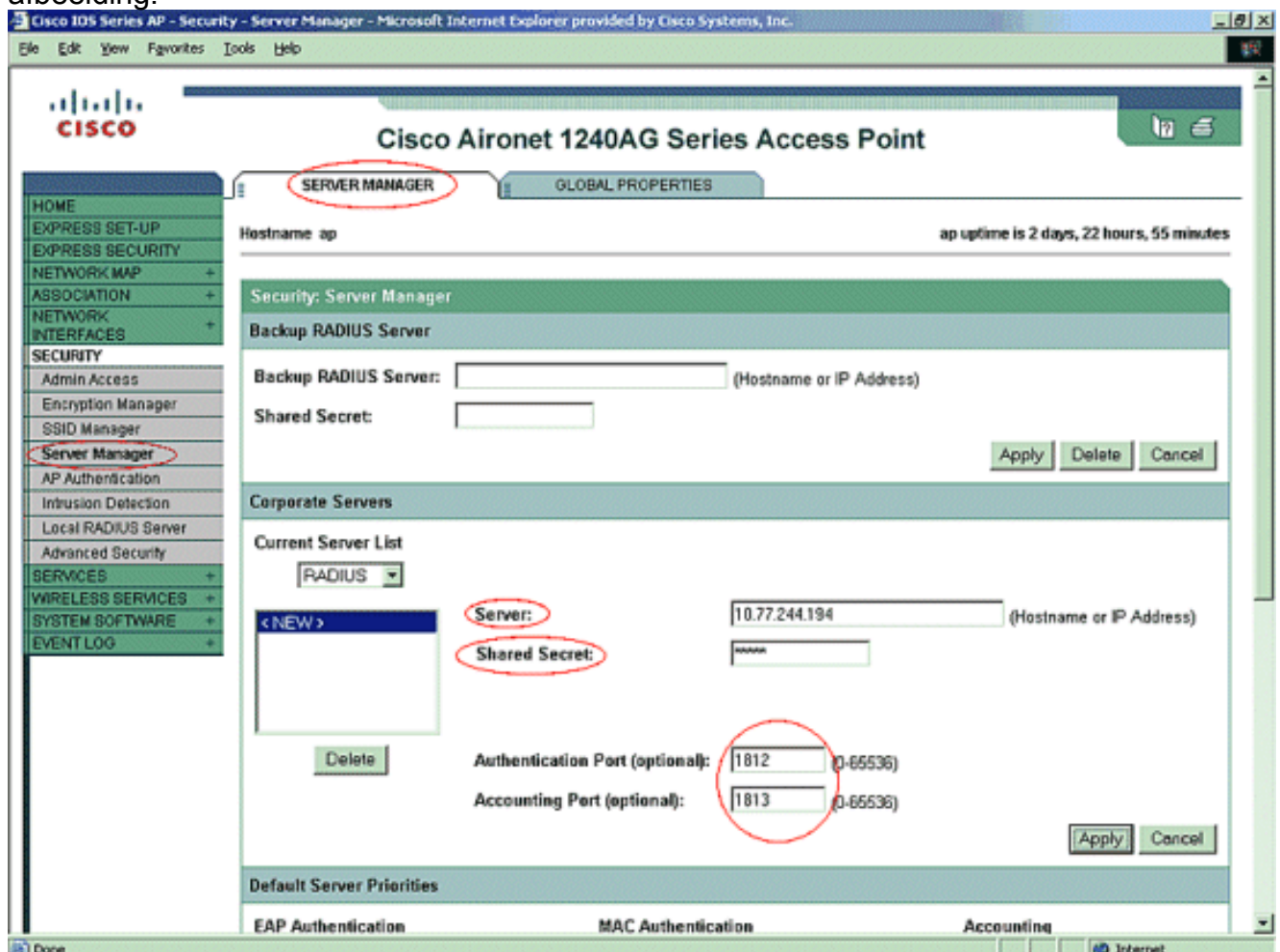
server host 10.77.244.194 auth-port 1812 acct-port
1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip !! line con 0
line vty 5 15 ! end

```

GUI-configuratie

Voltooi deze stappen om de functie Local RADIUS Server met de GUI te configureren:

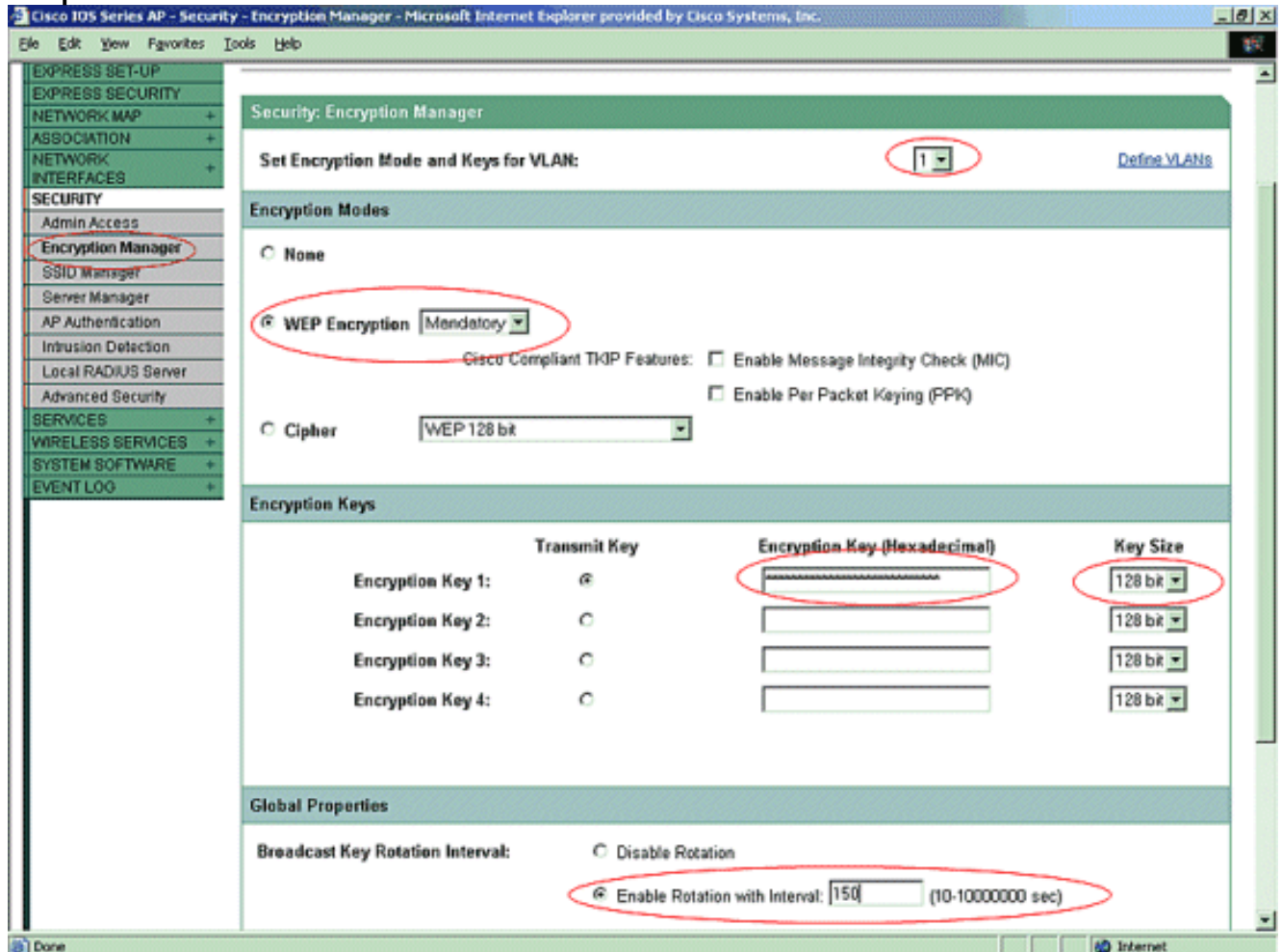
1. Kies in het menu aan de linkerkant het tabblad Server Manager onder het menu Beveiliging. Configureer de server en vermeld het IP-adres van dit access point, dat in dit voorbeeld 10.77.244.194 is. Vermeld de poortnummers 1812 en 1813 waarop de Local Radius server luistert. Specificeer het gedeelde geheim dat met de lokale RADIUS-server moet worden gebruikt zoals in de afbeelding.



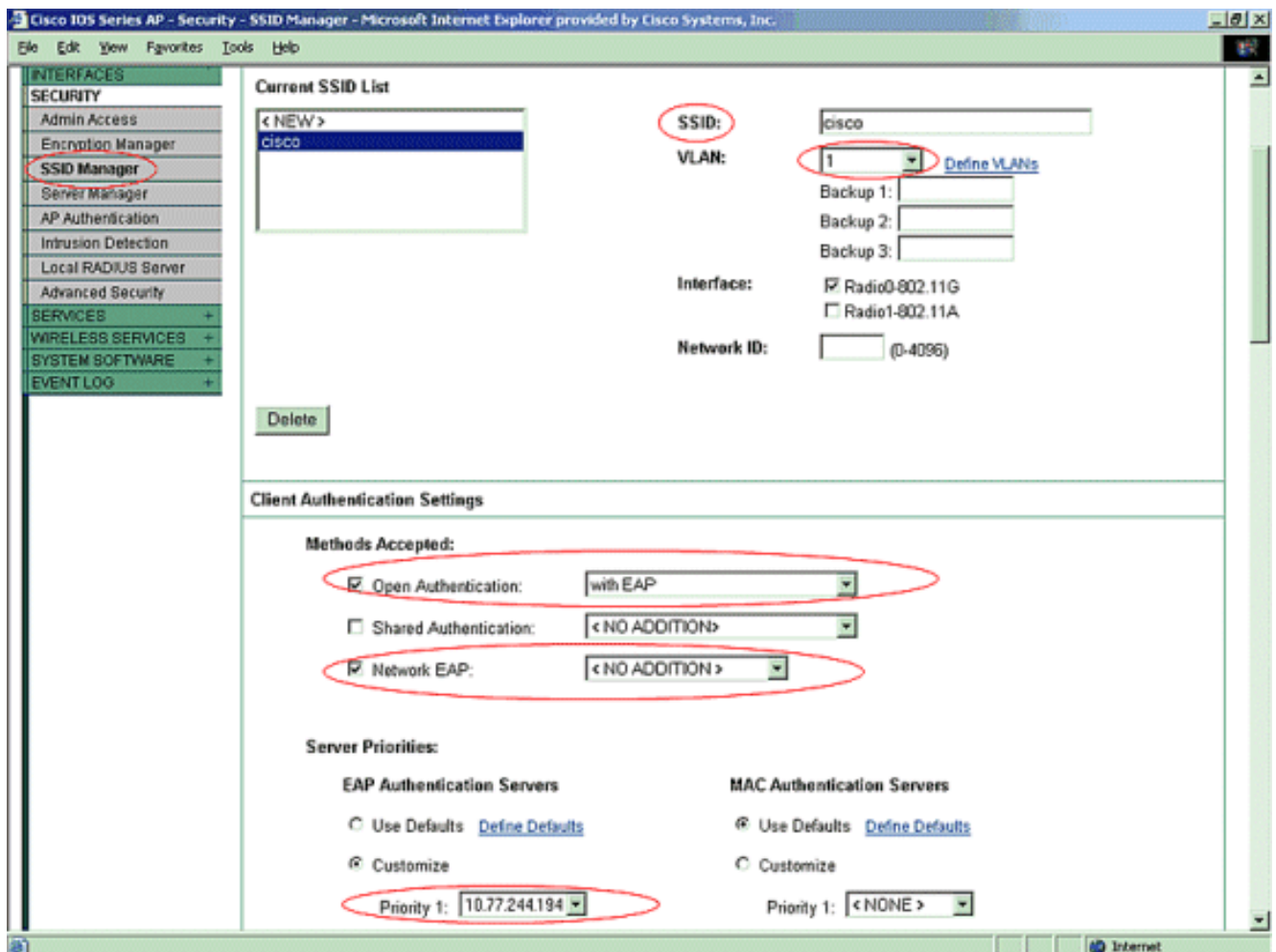
2. Klik in het menu aan de linkerkant op het tabblad Encryption Manager onder het menu Security. Specificeer de toe te passen VLAN. Specificeer dat de encryptie van EFN moet worden gebruikt. Specificeer dat het gebruik VERPLICHT is. Initialiseer elke sleutel van EFG met een hexadecimaal teken van 26 cijfers. Deze sleutel wordt gebruikt om uitzending en multicast pakketten te versleutelen. Deze stap is optioneel. Stel de sleutelgrootte in op 128 bits. U kunt ook 40 bits kiezen. In dit geval, moet de de zeer belangrijke grootte van EFN in de vorige stap een 10-cijferig hexadecimaal karakter zijn. Deze stap is optioneel. U kunt ook

omwenteling van de uitzending inschakelen en het tijdstip specificeren waarna de uitzending-toets wordt gewijzigd. Als deze uitgeschakeld is, wordt de uitgezonden toets nog gebruikt maar niet gewijzigd. Deze stap is optioneel. **Opmerking:** Deze stappen worden herhaald voor elk VLAN dat LEAP-verificatie gebruikt. Klik op

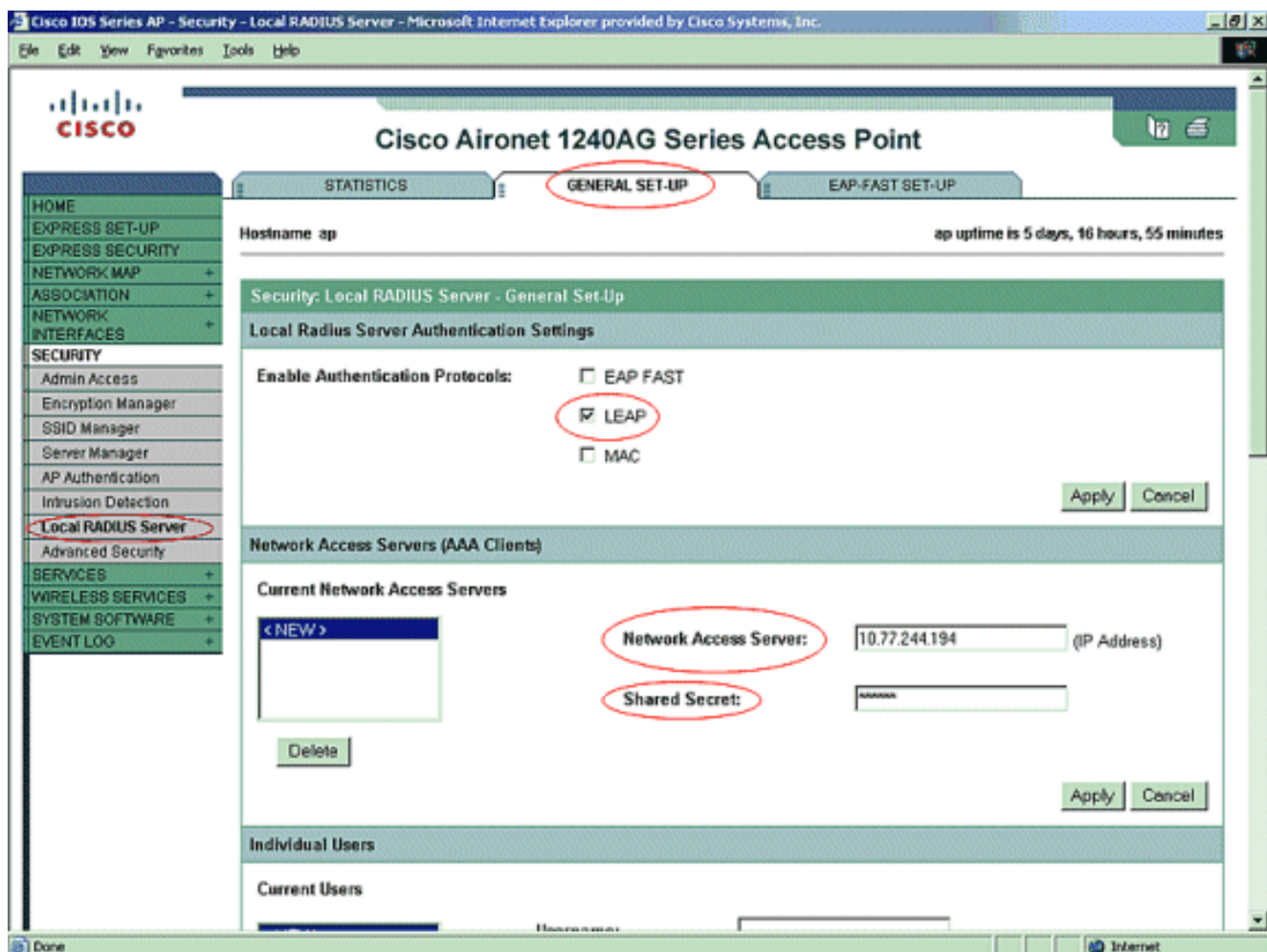
Toepassen.



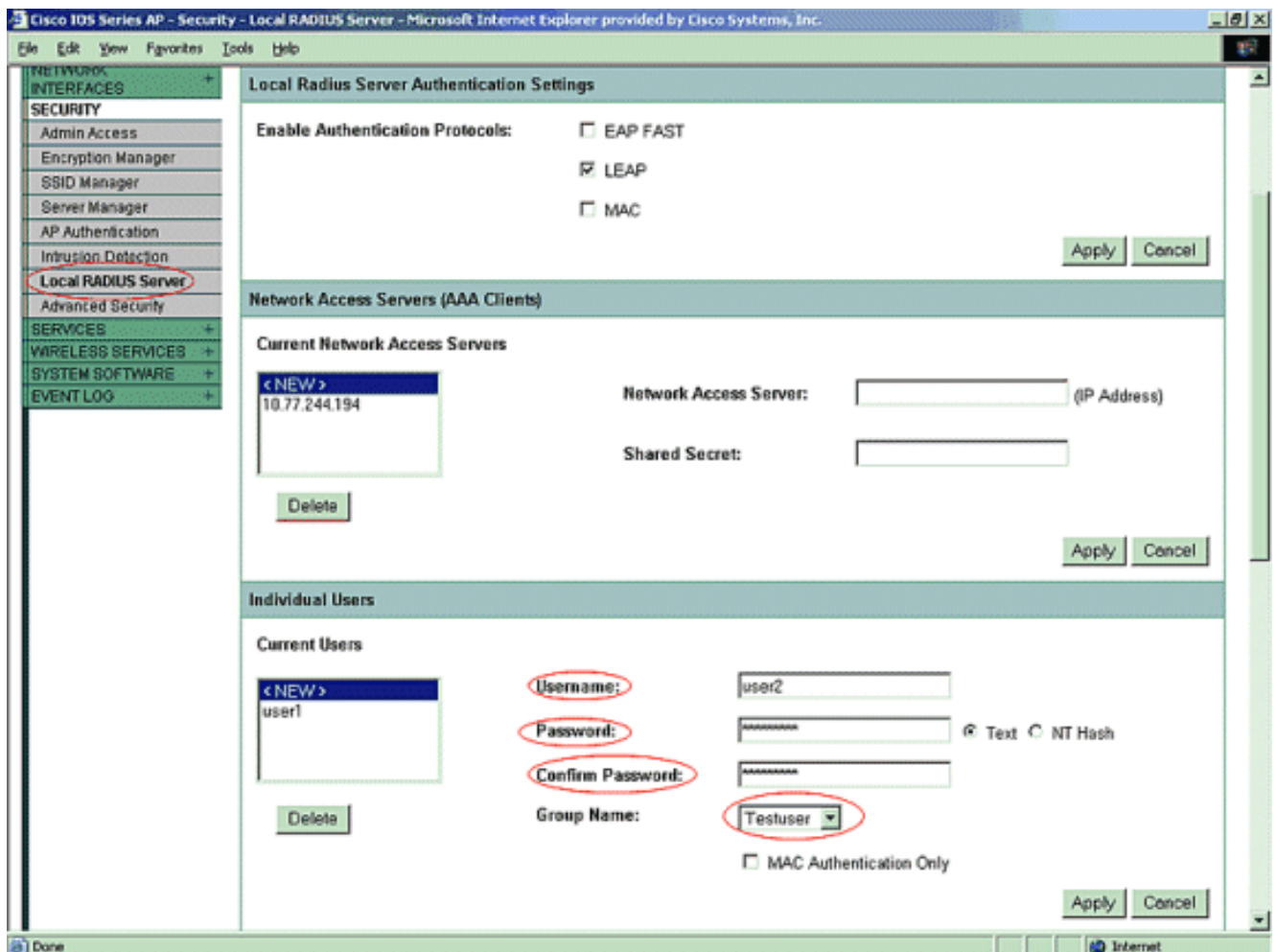
- Voer in het menu Beveiliging van het tabblad SSID Manager deze handelingen uit: **Opmerking:** U kunt later aanvullende functies en sleutelbeheer toevoegen als u hebt bevestigd dat de basisconfiguratie correct werkt. Definieer een nieuwe SSID en associeer het met een VLAN. In dit voorbeeld wordt SSID geassocieerd met VLAN 1. Controleer **Open verificatie (met EAP)**. Controleer **netwerk EAP (geen toevoeging)**. Kies uit **serverprioriteiten > EAP-verificatieservers** voor **aanpassen**; kies het IP-adres van dit access point voor **prioriteit 1**. Klik op **Toepassen**.



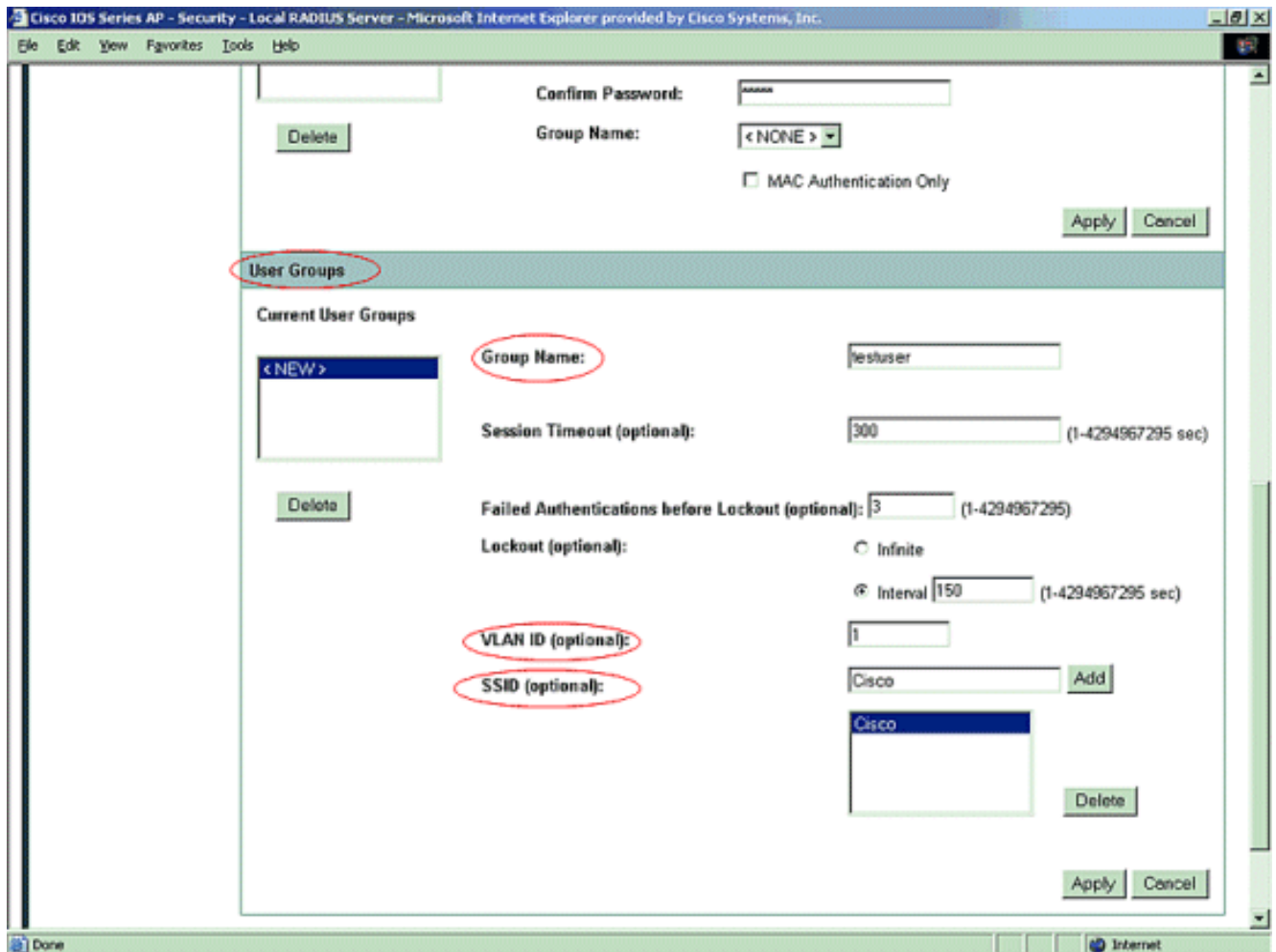
4. Klik onder Beveiliging op Local RADIUS Server in het tabblad General Set-UP. Onder Local Radius Server Authentication Settings controleert LEAP om zeker te zijn dat de LEAP-verificatieverzoeken worden aanvaard. Bepaal het IP-adres en het gedeelde geheim van de RADIUS-server. Voor Local RADIUS Server is dit het IP-adres van deze AP (10.77.244.194). Klik op Toepassen.



5. Scrollt neer van de Lokale Server van RADIUS onder het tabblad Algemene instelling en definieer de individuele gebruikers met hun gebruikersnamen en wachtwoorden. Opties, kunnen gebruikers worden gekoppeld aan groepen, die in de volgende stap worden gedefinieerd. Dit zorgt ervoor dat alleen bepaalde gebruikers zich aanmelden bij een SSID.**Opmerking:** De lokale RADIUS-database bestaat uit deze individuele gebruikersnamen en wachtwoorden.



6. Scrollt verder naar beneden op dezelfde pagina, opnieuw van de lokale RADIUS-server onder het subtabblad Algemene instelling naar gebruikersgroepen. definieert gebruikersgroepen en koppelt ze aan een VLAN of SSID.



Opmerking: Groepen zijn optioneel. De groeieigenschappen geven niet over aan Actieve Map en zijn alleen lokaal relevant. U kunt groepen later toevoegen, nadat u hebt bevestigd dat de basisconfiguratie correct werkt.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

- **Straal lokaal-server statistieken**-Deze opdracht toont statistieken die door de lokale authenticator worden verzameld.

```

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

```

- **Straalserver-groep all**-Deze opdracht toont een lijst van alle geconfigureerde RADIUS-servergroepen op het access point.

Problemen oplossen

Procedure voor probleemoplossing

Deze sectie verschaft informatie over probleemoplossing die relevant is voor deze configuratie.

1. Om de mogelijkheid van RF-emissies die succesvolle authenticatie beletten uit te sluiten, stelt u de methode op de SSID in om de verificatie tijdelijk uit te schakelen. Schakel in de GUI op de pagina van SSID Manager de **MAP-netwerkopties uit** en **open** controleren. Van de opdrachtregel—gebruik de opdrachten **authenticatie open** en **geen authenticatie netwerk-eap_methods**. Als de cliënt met succes geassocieerd is, draagt RF niet bij aan het associatieprobleem.
2. Controleer dat alle gedeelde geheime wachtwoorden gesynchroniseerd zijn. De lijnen `straal-server host x.x.x.x.x auth-port x acct-port x key <Shared_geheime> en nas x.x.x.x sleutel <gedeeld_geheim>` moeten hetzelfde gedeelde geheime wachtwoord bevatten.
3. Verwijder eventuele gebruikersgroepen en configuratie van gebruikersgroepen. Soms kunnen er conflicten ontstaan tussen gebruikersgroepen die gedefinieerd zijn door het toegangspunt en gebruikersgroepen die binnen het domein actief zijn.

Opdrachten voor probleemoplossing

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

- **debug dot11 a authenticator all** - Dit debug toont de verschillende onderhandelingen die een client doorvoert als de client associeert en authenticaceert door het 802.1x of EAP proces vanuit het perspectief van Authenticator (Access Point). Dit debug werd geïntroduceerd in Cisco IOS-software release 12.2(15)JA. Deze opdracht vervalt debug dot11 a dot1x in dat en laat vrijkomen.

```
*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 straal authenticatie**-Dit debug toont de RADIUS onderhandelingen tussen de server en client, die in dit geval allebei het toegangspunt zijn.
- **debug Straal client-server**-Dit debug toont de authenticatie van de client vanuit het perspectief van de RADIUS-server.

```

*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 1 00:30:00.756: 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]

```

- **bug van lokale serverpakketten** - Deze debug toont alle processen die door en vanuit het perspectief van de RADIUS-server zijn uitgevoerd.

[Gerelateerde informatie](#)

- [Een access point configureren als lokale verificator](#)
- [Verificatietypen configureren](#)
- [RADIUS- en TACACS+ servers configureren](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)