

Configuratievoorbeeld van H-REAP-modi van bediening

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[H-REAP via REAP](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[De AP met een controller voorbereiden en H-REAP configureren](#)

[H-REAP-overzicht van bewerkingen](#)

[H-REAP-switchingstaten](#)

[Central-verificatie, Central-switching](#)

[Controleer de Central-verificatie, Central-switching](#)

[Verificatie omlaag, switching omlaag](#)

[Central-verificatie, lokale switching](#)

[Controleer de centrale verificatie, lokale switching](#)

[Verificatie beneden, lokale switching](#)

[Lokale verificatie, lokale switching](#)

[Controleer lokale verificatie, lokale switching](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document introduceert het concept Hybrid Remote Edge Access Point (H-REAP) en legt de verschillende werkingsmodi uit met een voorbeeldconfiguratie.

Voorwaarden

Vereisten

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

- Kennis van draadloze LAN-controllers (WLC's) en hoe u de WLC-fundamentele parameters

- kunt configureren
- Kennis van REAP

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4400 Series WLC-software met firmware release 7.0.16.0
- Cisco Aironet 1131AG lichtgewicht access point (LAP)
- Cisco 2800 Series routers die versie 12.4(11)T uitvoeren.
- Cisco Aironet 802.11a/b/g clientadapter voor firmware release 4.0
- Cisco Aironet desktop Utility versie 4.0
- Cisco Secure ACS dat versie 4.0 ondersteunt

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.](#)

Achtergrondinformatie

H-REAP is een draadloze oplossing voor bijkantoor en externe kantoorimplementaties. H-REAP stelt klanten in staat om toegangspunten (APs) in een tak of ver bureau van het bedrijfsbureau door een WAN verbinding te vormen en te controleren zonder in elk bureau een controller te implementeren.

H-REAPs kan clientgegevensverkeer lokaal switches en lokale clientverificatie uitvoeren wanneer de verbinding met de controller verloren gaat. H-REAP's kunnen ook tunnelverkeer naar de controller uitvoeren wanneer zij worden aangesloten op de controller. In de aangesloten modus kan de hybride REAP ook lokale authenticatie uitvoeren.

H-REAP wordt alleen ondersteund op:

- 1130AG, 1140, 1240, 1250, 1260, AP801, AP802, 1040, en AP3550 APs
- Cisco 5500, 4400, 2100, 2500 en Flex 7500 Series controllers
- Catalyst 3750G geïntegreerde controller-Switch
- Catalyst 6500 Series draadloze servicesmodule (WiSM)
- Draadloze LAN-controllermodule (WLCM) voor geïntegreerde services routers (ISR's)

Het clientverkeer op H-REAP's kan lokaal worden geschakeld via de AP of worden teruggezet naar een controller. Dit is afhankelijk van de configuratie per WLAN. Tevens kan het lokaal geschakelde clientverkeer op de H-REAP worden gelabeld op 802.1Q voor een bekabelde scheiding. Tijdens WAN-outage blijft de service op alle lokaal switched, lokaal geauthenticeerde WLAN's bestaan.

Opmerking: Als APs in H-REAP modus zijn en lokaal op de verre plaats zijn geschakeld, wordt de

dynamische toewijzing van gebruikers aan een specifiek VLAN gebaseerd op de RADIUS serverconfiguratie niet ondersteund. U kunt echter gebruikers aan specifieke VLAN's toewijzen op basis van het statische VLAN aan de Service set identifier (SSID)-mapping (SSD) die lokaal bij de AP wordt uitgevoerd. Daarom kan een gebruiker die tot een bepaalde SSID behoort aan een specifiek VLAN worden toegewezen waaraan SSID lokaal bij AP in kaart wordt gebracht.

Opmerking: Als spraak via WLAN belangrijk is, moeten APs in lokale modus worden uitgevoerd zodat zij CCKM en Connection Admission Control (CAC) ondersteuning krijgen, die niet worden ondersteund in H-REAP-modus.

[H-REAP via REAP](#)

Raadpleeg het [Configuratievoorbeeld](#) van [Remote-Edge AP \(REAP\) met lichtgewicht AP's en draadloze LAN-controllers \(WLC's\)](#) voor meer informatie om REAP te begrijpen.

H-REAP werd ingevoerd als gevolg van deze tekortkomingen van REAP:

- REAP heeft geen draadscheiding. Dit komt door gebrek aan 802.1Q ondersteuning. Gegevens van de WLAN's landen op hetzelfde bekabelde subnet.
- Tijdens een WAN-storing stopt een REAP-applicatie de service die op alle WLAN's wordt aangeboden, behalve de eerste die in de controller is gespecificeerd.

Zo kan H-REAP deze twee tekortkomingen overwinnen:

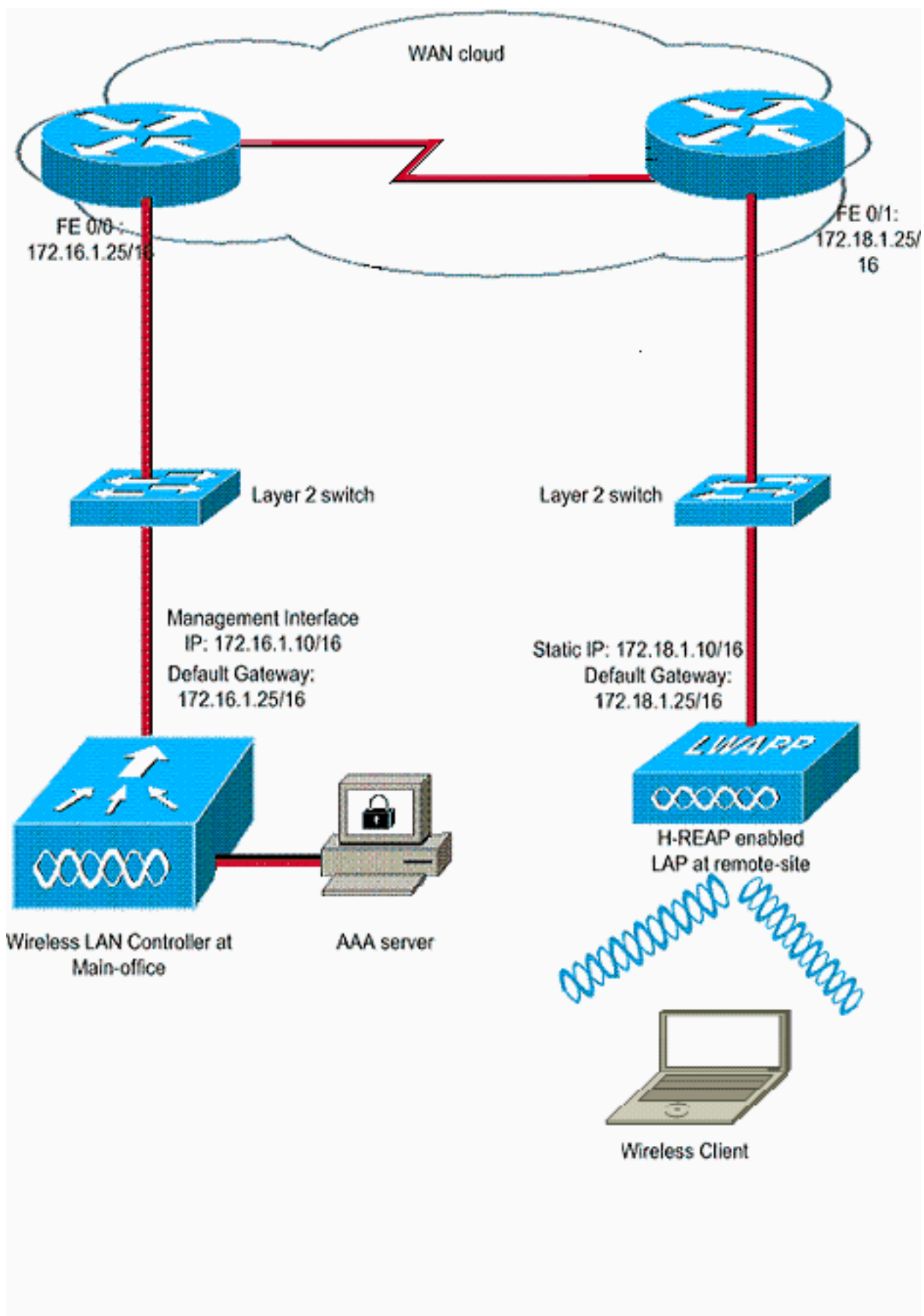
- Biedt dot1Q ondersteuning en VLAN aan SSID mapping. Dit VLAN aan SSID mapping moet bij H-REAP worden uitgevoerd. Wanneer u dit uitvoert, zorg er dan voor dat de geconfigureerd VLAN's correct door de poorten in intermediaire switches en routers zijn toegestaan.
- Biedt continue service aan alle WLAN's die voor lokale switching zijn geconfigureerd.

[Configureren](#)

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

[Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd:



Configuratie

In dit voorbeeld wordt ervan uitgegaan dat de controller al is ingesteld met basisconfiguraties. De controller gebruikt deze configuraties:

- IP-adres van beheerinterface 172.16.1.10/16
- AP-Manager interface IP-adres-172.16.1.11/16
- Standaard gateway voor IP-adres-172.16.1.25/16
- Virtual Gateway IP-adres-1.1.1.1

N.B.: Dit document bevat geen WAN-configuraties en geen configuratie van routers en switches die beschikbaar zijn tussen de H-REAP en de controller. Dit veronderstelt dat u van de insluiting van WAN en de routeringsprotocollen op de hoogte bent die worden gebruikt. Dit document gaat er ook van uit dat u begrijpt hoe u deze kunt configureren om de connectiviteit tussen de H-REAP en de controller te behouden via de WAN-link. In dit voorbeeld wordt de insluiting van HDLC op de WAN-link gebruikt.

[De AP met een controller voorbereiden en H-REAP configureren](#)

Als u wilt dat AP een controller van een extern netwerk ontdekt waar geen CAPWAP ontdekkingsmechanismen beschikbaar zijn, kunt u priming gebruiken. Met deze methode kunt u de controller specificeren waarmee de AP verbinding moet maken.

Om een AP-ReAP-Geslacht te in werking te stellen van H-REAP, sluit AP aan op het draadnetwerk op het hoofdbureau. Tijdens het opstarten van het programma zoekt de H-REAP-Geslacht AP eerst naar een IP adres voor zichzelf. Nadat het een IP-adres via een DHCP-server heeft aangeschaft, start het programma op en zoekt het naar een controller om het registratieproces uit te voeren.

Een H-REAP kan het controller IP-adres leren op een van de manieren die worden uitgelegd in [lichtgewicht AP \(LAP\)-registratie naar een draadloze LAN-controller \(WLC\)](#).

Opmerking: U kunt de LAP ook configureren om de controller te ontdekken via CLI-opdrachten bij de AP. Raadpleeg de [H-REAP Controller-ontdekking met CLI-opdrachten](#) voor meer informatie.

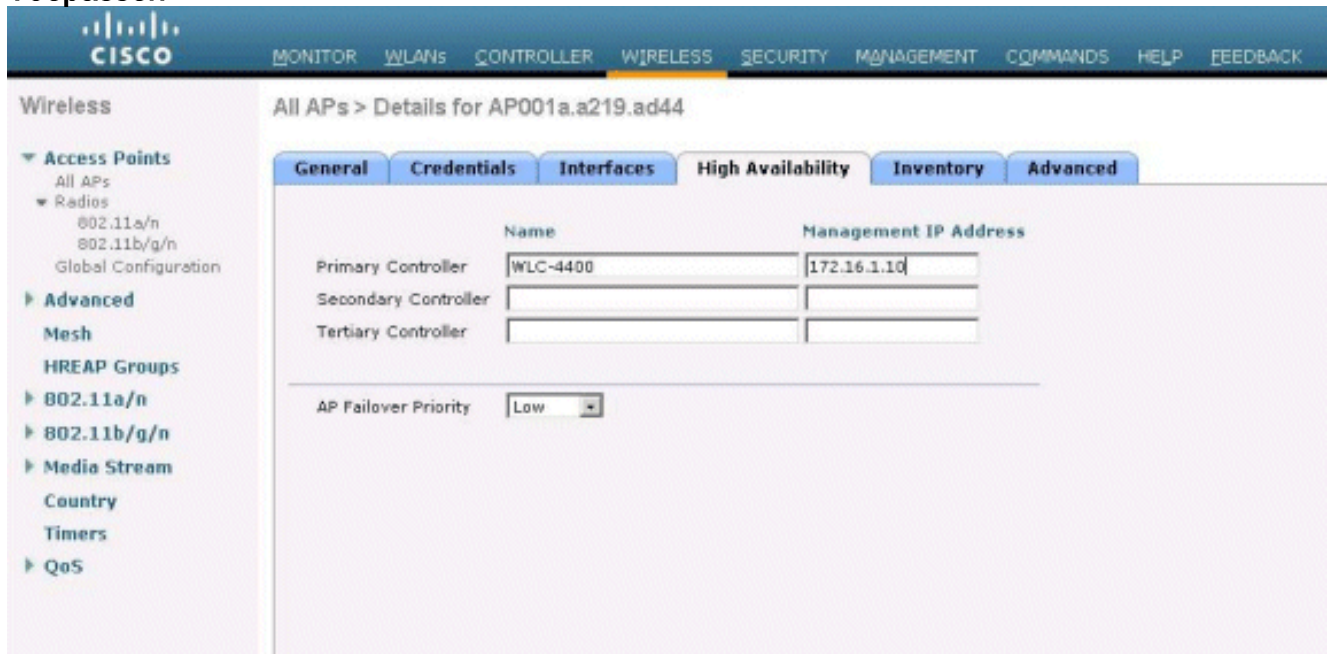
Het voorbeeld in dit document gebruikt de DHCP optie 43 procedure voor de H-REAP om het IP-adres van de controller te leren. Hiermee sluit u zich aan bij de controller, downloads van het laatste softwarebeeld en de configuratie van de controller, en initialiseert u de radiolink. Hiermee slaat u de gedownload configuratie op in niet-vluchtig geheugen, voor gebruik in de standalone modus.

Voltooi de volgende stappen zodra de LAP bij de controller is geregistreerd:

1. Kies in de Controller GUI **Wireless>Access points**. Hier wordt de LAP weergegeven die bij deze controller is geregistreerd.
2. Klik op de AP die u wilt configureren.

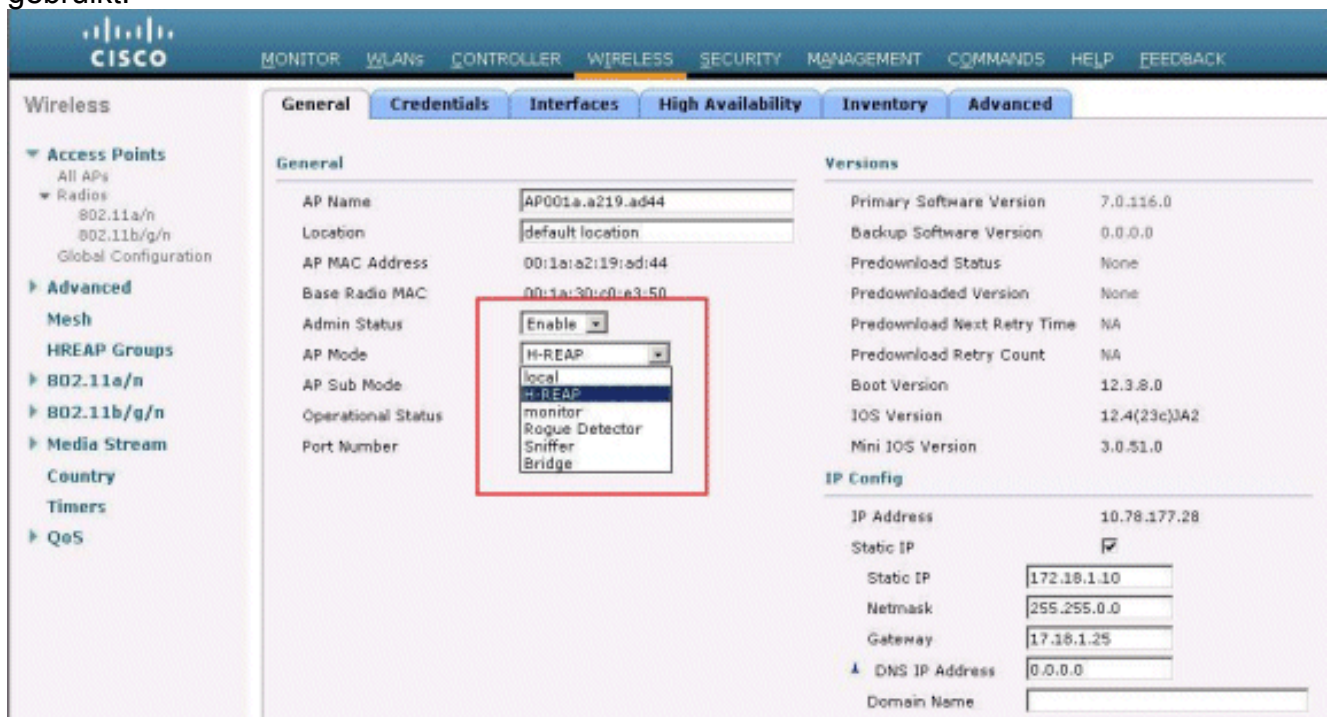
AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP001a-a219-a04d	AIR-LAP1131AG-A-K9	00:1e:a2:19:a0:4d	0 d, 00 h 06 m 12 s	Enabled	REG

- Klik in het venster APs>Details op het tabblad Hoge beschikbaarheid en definieer de controllernamen die de APs zullen gebruiken om te registreren en klik vervolgens op **Toepassen**.



U kunt maximaal drie controlerenamen definiëren (primair, secundair en tertiair). De APs zoeken naar de controller in de dezelfde volgorde die u in dit venster geeft. Omdat dit voorbeeld slechts één controller gebruikt, definieert het voorbeeld de controller als de primaire controller.

- LET configureren voor H-REAP. Om de LAP te configureren en in de H-REAP-modus te werken, kiest u in het venster APs>Details onder het tabblad Algemeen de **AP-modus** als H-REAP in het corresponderende uitrolmenu. Hiermee wordt de LAP ingesteld die in de H-REAP-modus moet worden gebruikt.



Opmerking: In dit voorbeeld, kunt u zien dat het IP-adres van het AP wordt gewijzigd in statische modus en dat het statische IP-adres 172.18.1.10 is toegewezen. Deze opdracht komt voor omdat dit het subtype is dat gebruikt moet worden op het externe kantoor. Daarom

gebruikt u het IP-adres vanuit de DHCP-server, maar alleen tijdens de eerste fase door het registratiefase. Nadat het AP bij de controller is geregistreerd, wijzigt u het adres in een statisch IP-adres.

Nu uw LAP is voorbereid met de controller en is geconfigureerd voor de H-REAP-modus, is de volgende stap om H-REAP aan de controller-kant te configureren en de H-REAP-switching staten te bespreken.

H-REAP-overzicht van bewerkingen

De H-REAP-compatibele LAP werkt in deze twee verschillende modi:

- **Verbonden** modus: Een H-REAP zou in aangesloten modus zijn wanneer zijn CAPWAP besturingsplane link naar de WLC omhoog en in gebruik is. Dit betekent dat de WAN-verbinding tussen de LAP en de WLC niet is verbroken.
- **Standalone**: Een H-REAP zou in de standalone modus zijn wanneer zijn WAN-verbinding met de WLC is gezakt. Bijvoorbeeld, wanneer deze H-REAP niet langer connectiviteit op de WLC verbonden over de WAN verbinding heeft.

Het echtheidsmechanisme dat wordt gebruikt om een cliënt te authenticeren kan worden gedefinieerd als **Centrale** of **Plaatselijke cliënten**.

- **Centrale Verificatie**—verwijst naar het authenticatietype dat het proces van de WLC van de verafgelegen site betreft.
- **Lokale verificatie**—verwijst naar de authenticatietypen waarbij geen verwerking van de WLC voor verificatie is vereist.

Opmerking: alle 802.11 verificatie- en associatieverwerking vindt plaats bij de H-REAP, ongeacht de modus waarin de LAP zich bevindt. Terwijl in verbonden modus, geeft H-REAP deze associaties en authenticaties aan de WLC weer. In de standalone modus kan de LAP de WLC niet van dergelijke gebeurtenissen op de hoogte stellen.

Wanneer een client verbinding maakt met een H-REAP, stuurt AP alle authenticatieberichten door naar de controller. Nadat de verificatie is voltooid, worden de gegevenspakketten lokaal geschakeld of teruggezet naar de controller. Dit is in overeenstemming met de configuratie van het WLAN waarmee het is verbonden.

Met H-REAP kunnen de WLAN's die op een controller zijn geconfigureerd in twee verschillende modi worden gebruikt:

- **Central-switching**: Een WLAN-on H-REAP wordt verzonden naar een centrale switchmodus als het gegevensverkeer van die WLAN is geconfigureerd om naar de WLC te worden afgestemd.
- **Local Switching**: Een WLAN-on H-REAP wordt verzonden naar een lokale switchmodus als het gegevensverkeer van die WLAN lokaal bij de bekabelde interface van de LAP zelf eindigt, zonder dat dit wordt afgestemd op de WLC. **Opmerking:** Alleen WLAN's 1 tot en met 8 kunnen worden geconfigureerd voor H-REAP Local Switching, omdat alleen deze WLAN's kunnen worden toegepast op de 1130, 1240 en 1250 Series AP's die H-REAP-functionaliteit ondersteunen.

H-REAP-switchingstaten

In combinatie met de authenticatie- en switching-modi die in de voorgaande sectie worden genoemd, kan een H-REAP in elk van deze staten werken:

- [Central-verificatie, Central-switching](#)
- [Verificatie omlaag, switching omlaag](#)
- [Central-verificatie, lokale switching](#)
- [Verificatie beneden, lokale switching](#)
- [Lokale verificatie, lokale switching](#)

Central-verificatie, Central-switching

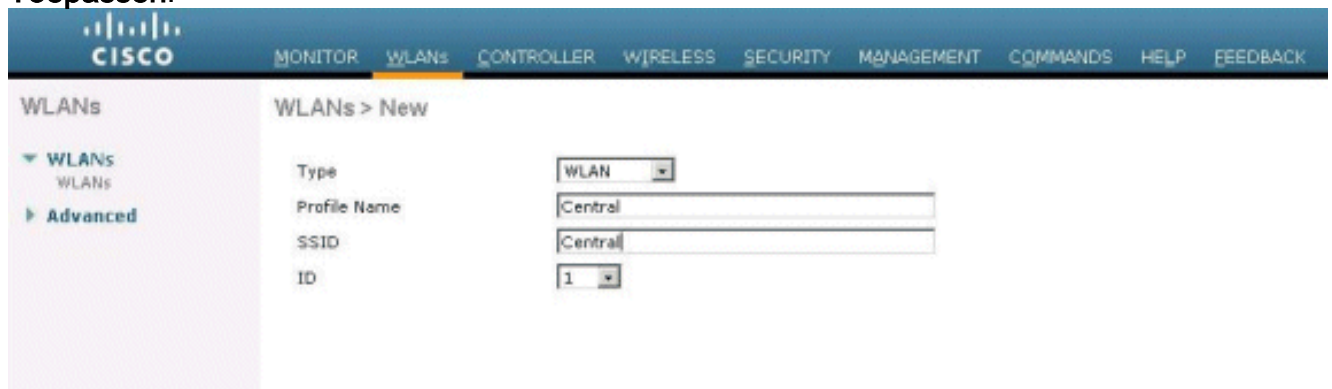
In deze staat, voor de gegeven WLAN, stuurt AP alle verzoeken van de clientverificatie door naar de controller en tunnels alle clientgegevens naar de WLC. Deze status is alleen geldig wanneer de H-REAP in de aangesloten modus staat. Alle WLAN's die zodanig zijn geconfigureerd dat ze in deze modus werken, worden verloren tijdens een WAN-uitgang, ongeacht de authenticatiemethode.

Dit voorbeeld gebruikt deze configuratie instellingen:

- WLAN/SSID-naam: **Centraal**
- Layer 2 security: **WAP2**
- Lokale switching: H-REAP **gehandicapt**

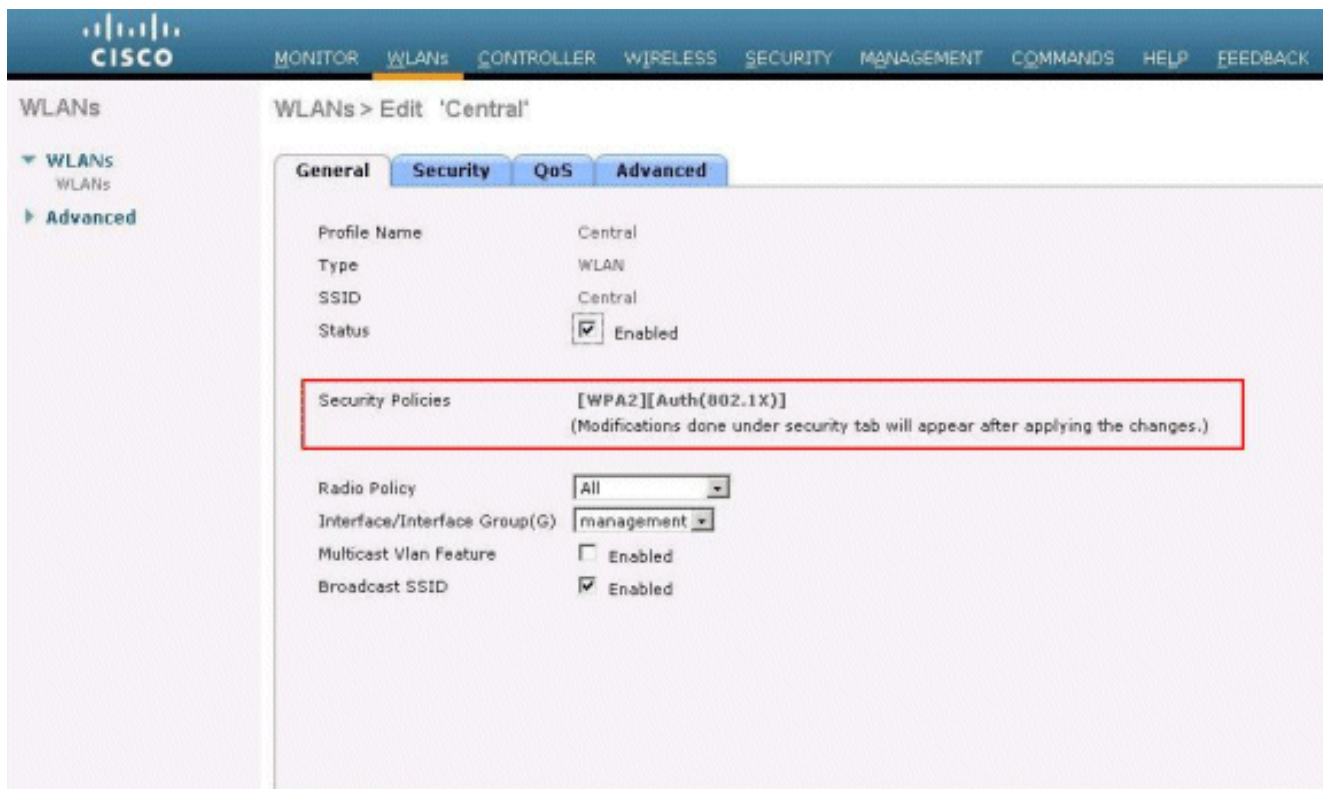
Voltooi deze stappen om de WLC voor centrale authenticatie te configureren, centrale switching met behulp van GUI:

1. Klik op **WLAN's** om een nieuw WLAN met de naam **Central** te maken, en klik vervolgens op **Toepassen**.

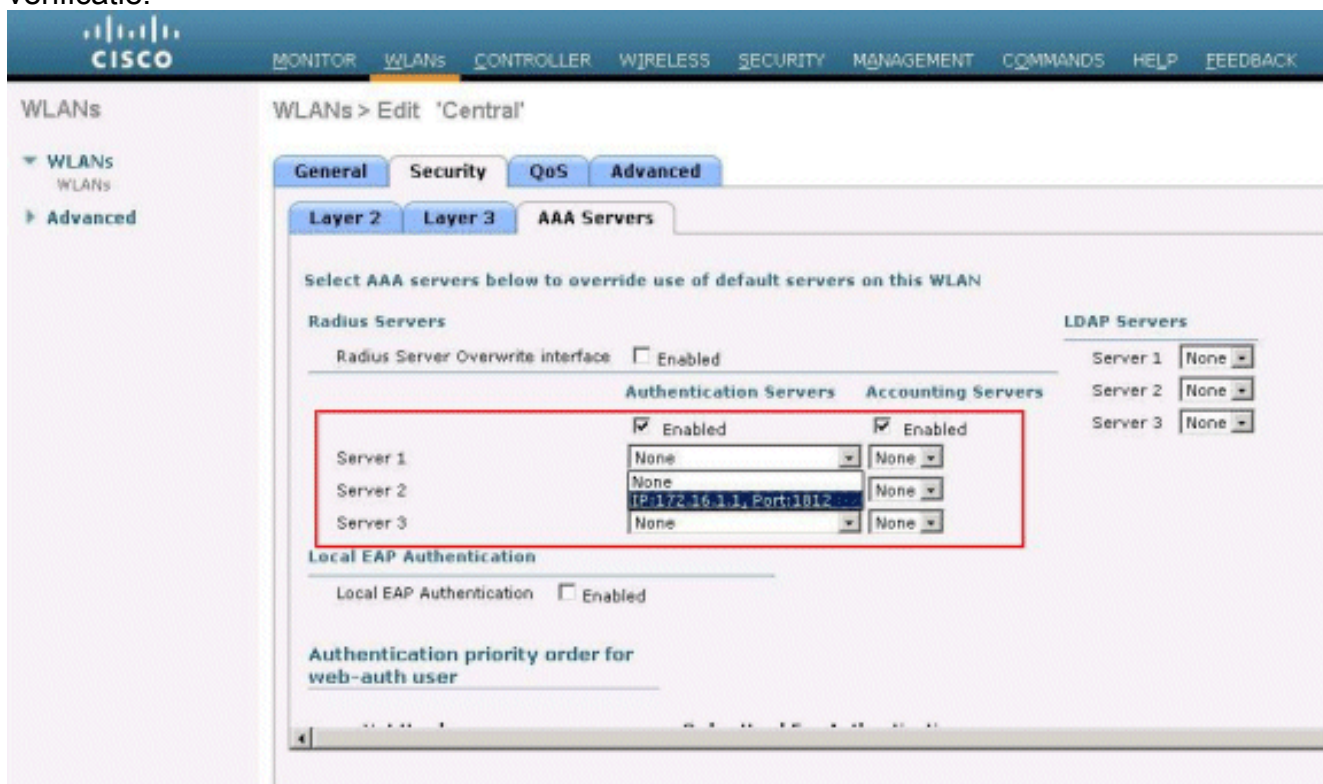


The screenshot shows the Cisco WLC GUI with the 'WLANs' tab selected. The 'WLANs > New' configuration page is displayed. The 'Type' dropdown menu is set to 'WLAN'. The 'Profile Name' field contains 'Central'. The 'SSID' field contains 'Central'. The 'ID' dropdown menu is set to '1'. The 'Advanced' option is selected in the left sidebar.

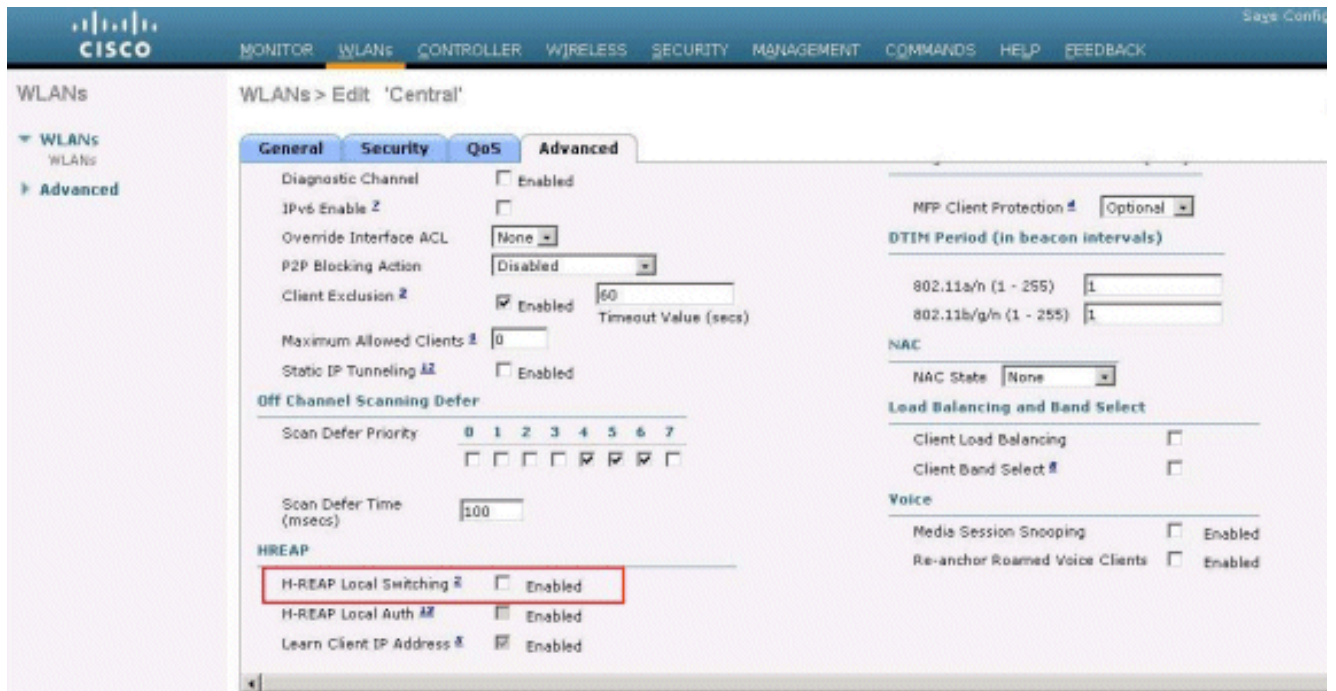
2. Omdat dit WLAN centrale verificatie gebruikt, gebruiken we WAP2-verificatie in het veld Layer 2 security. WAP2 is de standaard Layer 2 security voor een WLAN.



3. Kies het tabblad AAA-servers en kies vervolgens de juiste server die is ingesteld voor verificatie.



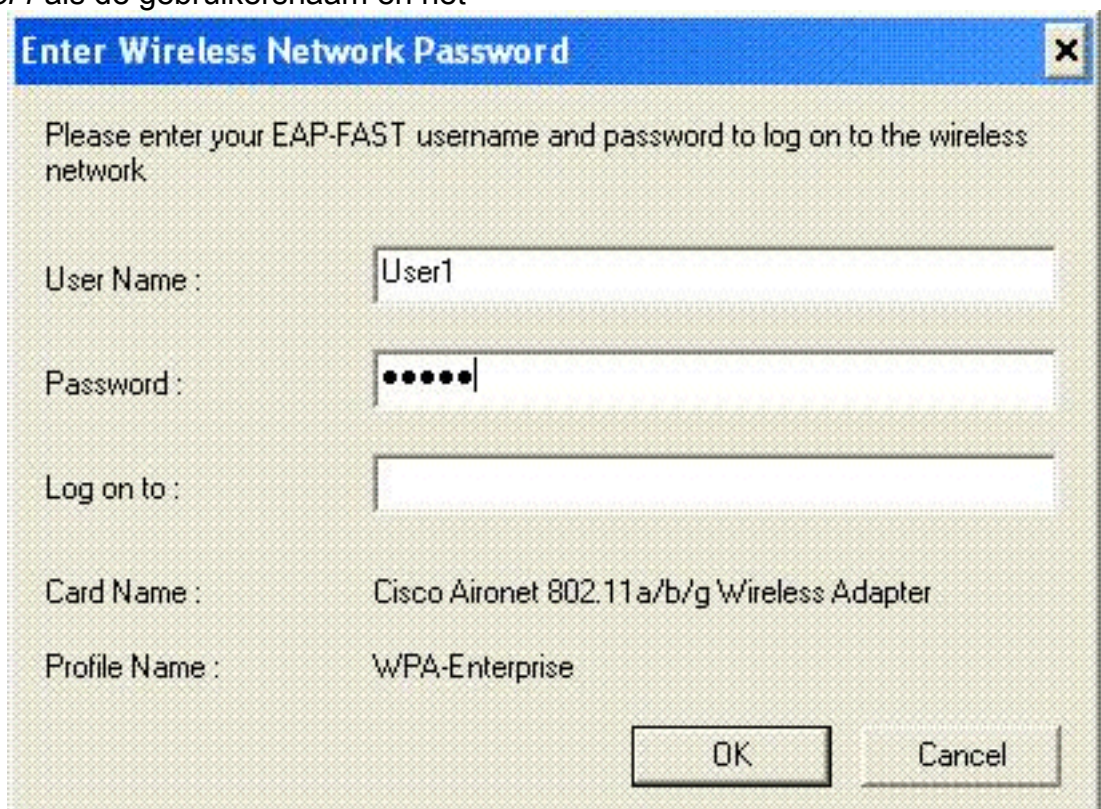
4. Omdat dit WLAN gebruik maakt van een centrale switching, moet u ervoor zorgen dat het aankruisvakje voor H-REAP Local Switching uitgeschakeld is (dit is een lokale switchingcontrole niet geselecteerd). Klik vervolgens op **Toepassen**.



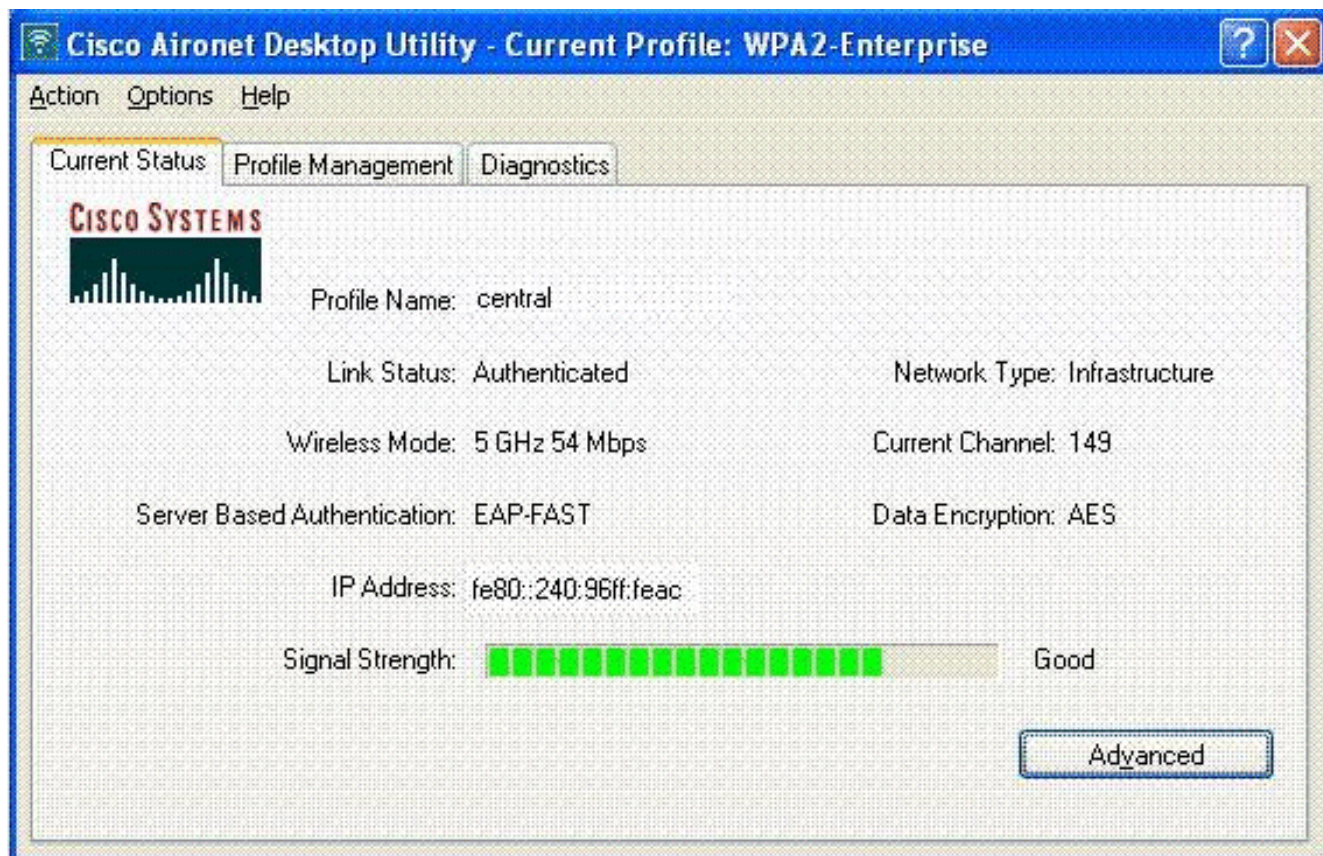
Controleer de Central-verificatie, Central-switching

Voer de volgende stappen uit:

1. Configureer de draadloze client met dezelfde SSID en beveiligingsconfiguraties. In dit voorbeeld is SSID *Central* en de veiligheidsmethode is *WAP2*.
2. Voer de gebruikersnaam en het wachtwoord in zoals ingesteld in de RADIUS-server > Instellingen gebruiker om de centrale SSID in de client te activeren. Dit voorbeeld gebruikt *User1* als de gebruikersnaam en het



wachtwoord. De client is centraal geauthentiseerd door de RADIUS-server en is gekoppeld aan de H-REAP. De H-REAP is nu in **centrale authenticatie, centrale omschakeling**.



[Verificatie omlaag, switching omlaag](#)

Omdat de zelfde configuratie in de [Centrale Verificatie, het](#) gedeelte Centrale [Switching](#), wordt verklaard, schakelt u de WAN-link uit die de controller verbindt. Nu wacht de controller op een hartstochtelijk antwoord van de AP. Een antwoord op de hartslag lijkt op boodschappen die levend blijven. De controller probeert vijf opeenvolgende hartslagen, elke seconde.

Omdat het niet ontvangen wordt met een hartstochtelijk antwoord van de H-REAP, dereguleert de WLC de LAP.

Laat de **debug capwap gebeurtenissen** uit zodat u opdracht krijgt van de CLI van de WLC om het deregistratieproces te controleren. Dit is de voorbeeldoutput van deze **debug** opdracht:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
```

Het H-REAP gaat naar de standalone modus.

Omdat dit WLAN eerder centraal geauthentiseerd en centraal switched was, werden zowel controle- als gegevensverkeer teruggezet naar de controller. Zonder controller kan de klant daarom geen associatie met de H-REAP onderhouden en is de verbinding verbroken. Deze status van H-REAP met zowel client associatie als authenticatie wordt aangeduid als verificatie Down, Switching Down.

Central-verificatie, lokale switching

In deze staat, voor het bepaalde WLAN, verwerkt WLC alle client authenticatie en de H-REAP LAP switches lokale gegevenspakketten. Nadat de client beveiligd is, stuurt de controller de opdrachten voor de controle van de kapWAP naar de H-REAP en geeft hij de LAP-instructies aan de switch van de gegevenspakketten van de client ter plaatse. Dit bericht wordt per cliënt verstuurd na succesvolle authenticatie. Deze status is alleen van toepassing in de aangesloten modus.

Dit voorbeeld gebruikt deze configuratie instellingen:

- WLAN/SSID-naam: **Centraal-lokaal**
- Layer 2 security: **WAP2**.
- Lokale switching: H-REAP **Ingeschakeld**

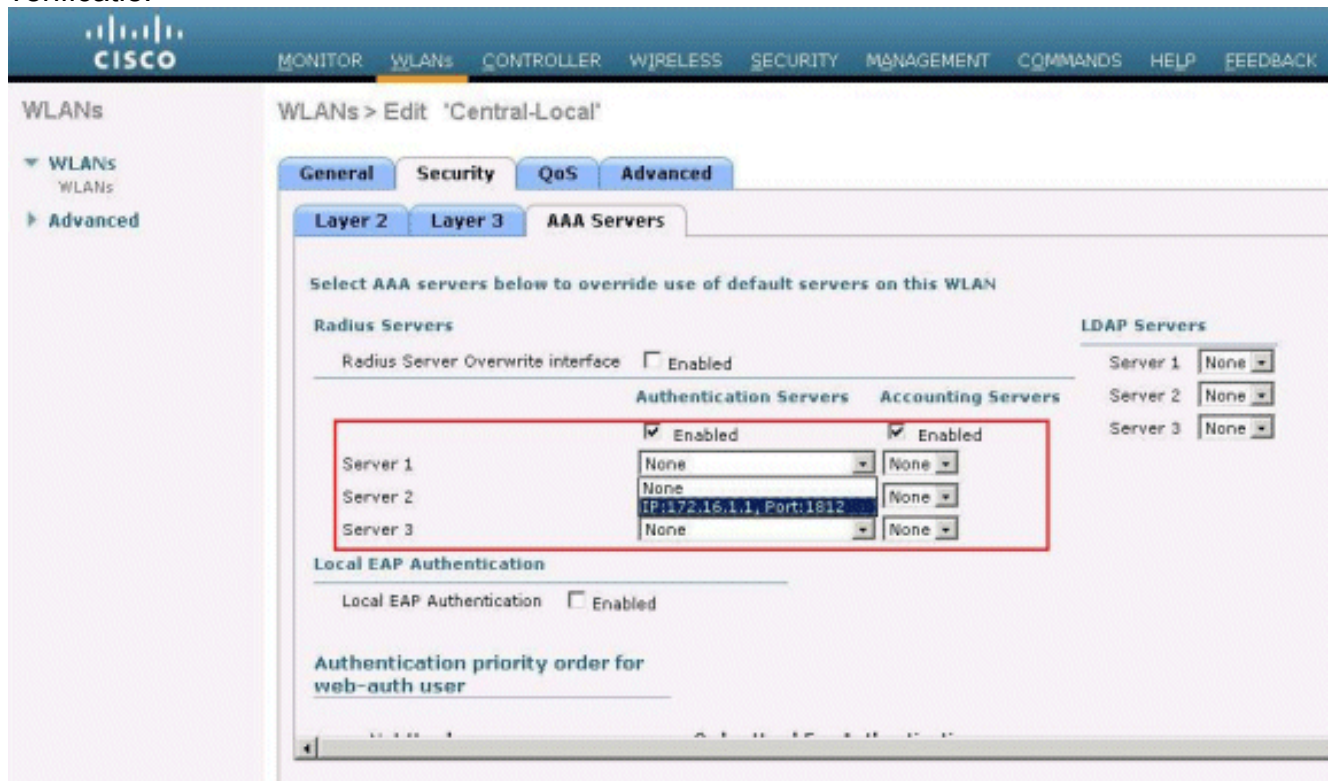
Voltooi de volgende stappen vanuit de GUI-controller:

1. Klik op **WLAN's** om een nieuw WLAN met de naam Central-Local te maken en klik vervolgens op **Toepassen**.
2. Omdat dit WLAN centrale verificatie gebruikt, kiest u **WAP2**-verificatie in het veld Layer 2 security.

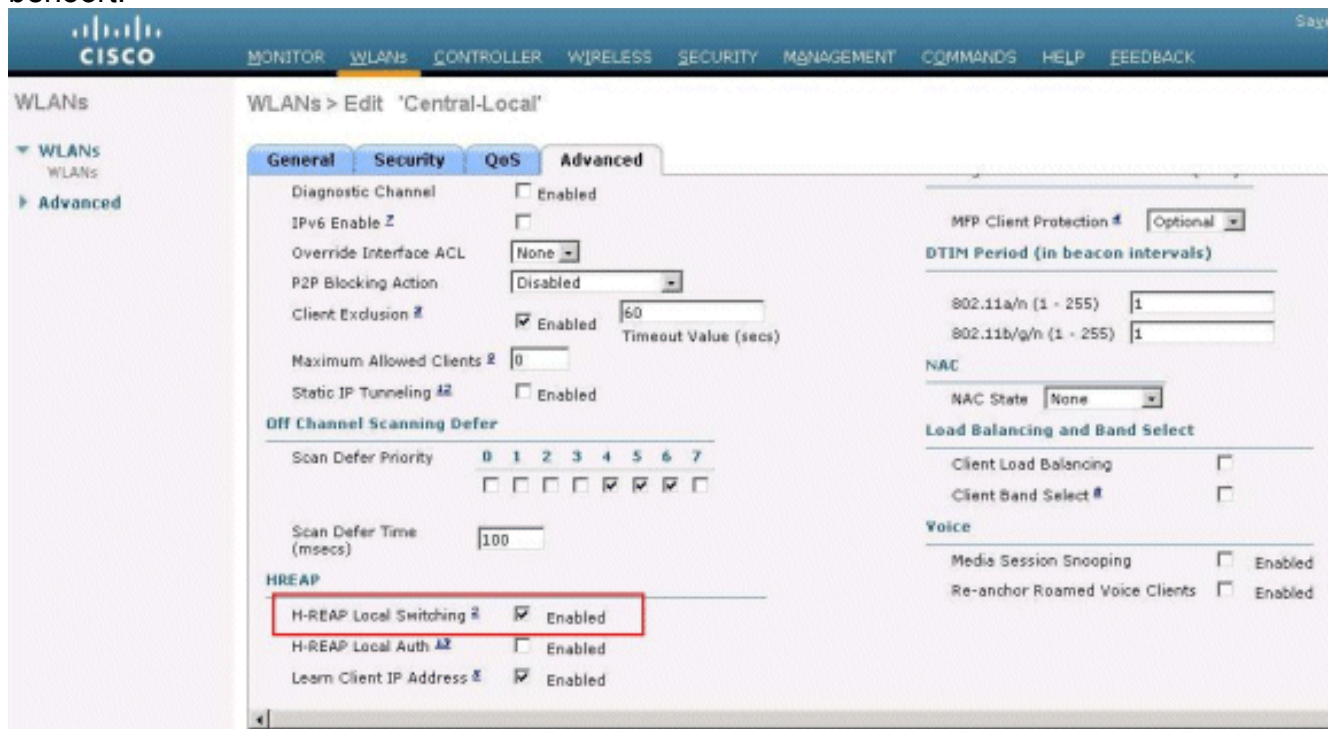
The screenshot shows the Cisco WLC GUI for editing a WLAN named 'Central-Local'. The 'Security' tab is active, and the 'Security Policies' field is highlighted with a red box, containing the text '[WPA2][Auth(802.1X)]'. Below this, a note states '(Modifications done under security tab will appear after applying the changes.)'. Other configuration options visible include Profile Name (Central-Local), Type (WLAN), SSID (Central-Local), Status (Enabled), Radio Policy (All), Interface/Interface Group(G) (management), Multicast Vlan Feature (Disabled), and Broadcast SSID (Enabled).

3. Kies onder het gedeelte Radius Server de juiste server die is ingesteld voor

verificatie.



4. Controleer het aanvinkvakje **H-REAP Local Switching** om het clientverkeer te switches dat lokaal bij de H-REAP aan dit WLAN behoort.



[Controleer de centrale verificatie, lokale switching](#)

Voer de volgende stappen uit:

1. Configureer de draadloze client met dezelfde SSID en beveiligingsconfiguraties. In dit voorbeeld is SSID *Central-Local* en de veiligheidsmethode is *WAP2*.
2. Voer de gebruikersnaam en het wachtwoord in zoals ingesteld in de RADIUS-

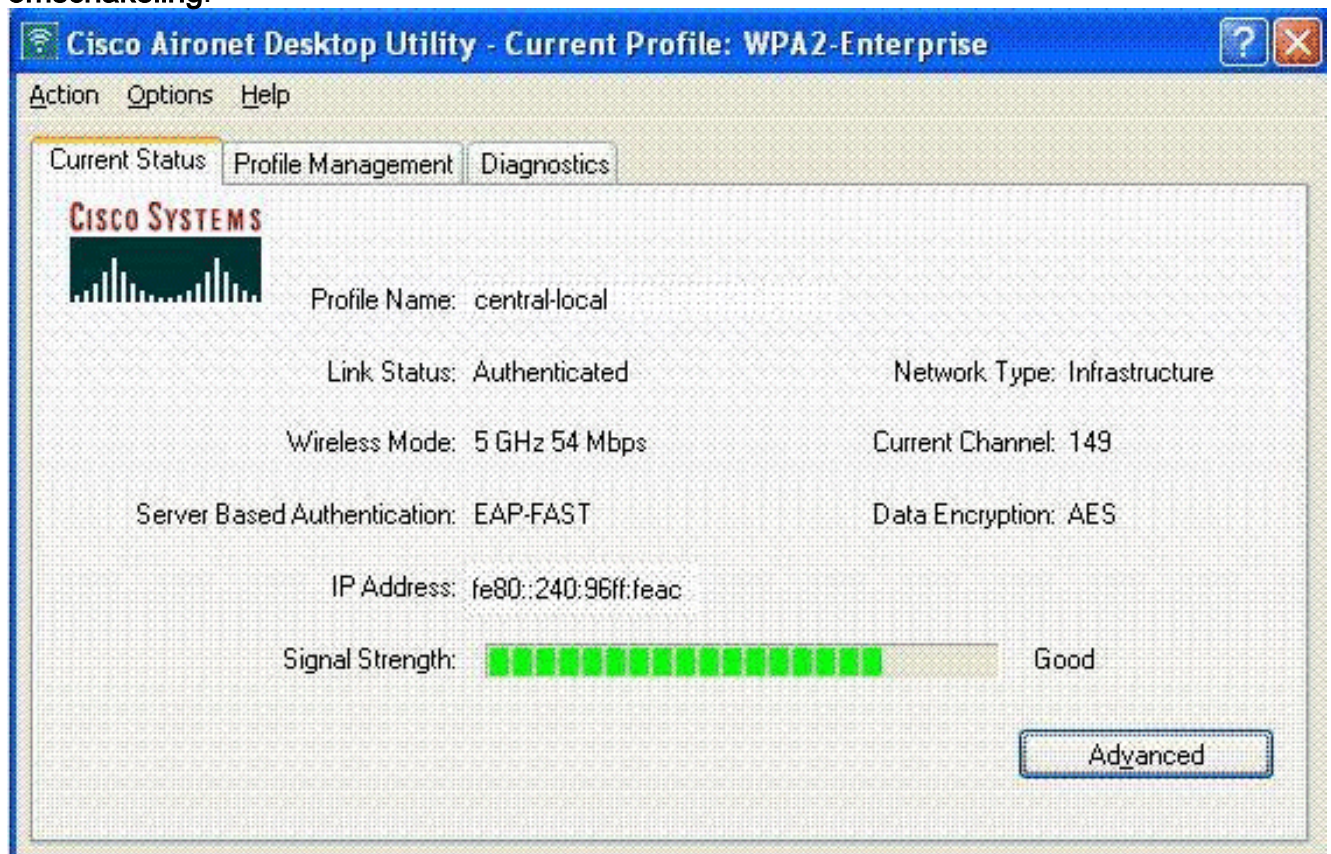
server>Gebruikersinstelling om de centrale-lokale SSID in de client te activeren.Dit voorbeeld gebruikt *User1* als de gebruikersnaam en het




The screenshot shows a dialog box titled "Enter Wireless Network Password". The text inside reads: "Please enter your EAP-FAST username and password to log on to the wireless network". There are three input fields: "User Name" containing "User1", "Password" containing six dots, and "Log on to" which is empty. Below the input fields, the "Card Name" is "Cisco Aironet 802.11 a/b/g Wireless Adapter" and the "Profile Name" is "WPA-Enterprise". At the bottom right, there are "OK" and "Cancel" buttons.

wachtwoord.

3. Klik op **OK**.De client is centraal geauthenticeerd door de RADIUS-server en wordt gekoppeld aan de H-REAP. De H-REAP is nu in **centrale authenticatie, lokale omschakeling**.



The screenshot shows the "Cisco Aironet Desktop Utility" window with the title "Current Profile: WPA2-Enterprise". The "Current Status" tab is selected. The Cisco Systems logo is visible. The status information is as follows:

Profile Name: central-local	Network Type: Infrastructure
Link Status: Authenticated	Current Channel: 149
Wireless Mode: 5 GHz 54 Mbps	Data Encryption: AES
Server Based Authentication: EAP-FAST	
IP Address: fe80::240:96ff:feac	
Signal Strength:  Good	

An "Advanced" button is located at the bottom right of the status area.

[Verificatie beneden, lokale switching](#)

Als een lokaal geschakeld WLAN is geconfigureerd voor elk verificatietype dat op WLC moet worden verwerkt (zoals EAP-verificatie [Dynamic/WAP/WAP2/802.11i], WebAuth, of NAC), wanneer WAN-falen, gaat dit de **verificatie naar beneden, de lokale** switching-status in. In deze staat, voor de gegeven WLAN, wijst de H-REAP elke nieuwe client af die probeert te authenticeren. De ECB blijft echter opmerkingen en enquêteresultaten sturen om bestaande cliënten goed met elkaar te verbinden. Deze status is alleen geldig in de standalone modus.

Om deze status te controleren gebruikt u dezelfde configuratie die is uitgelegd in de [Central Verificatie, Local Switching](#) sectie.

Als de WAN-link die de WLC met elkaar verbindt is neergedaald, gaat de WLC door het proces van deregulering van de H-REAP.

Als de H-REAP eenmaal is gedereguleerd, gaat hij over op een zelfstandige modus.

De client die door deze WLAN is gekoppeld, behoudt nog steeds zijn connectiviteit. Omdat de controller, de authenticator, echter niet beschikbaar is, staat H-REAP geen nieuwe verbindingen toe van dit WLAN.

Dit kan worden geverifieerd door de activering van een andere draadloze client in dezelfde WLAN. U kunt zien dat de authenticatie voor deze client mislukt en dat de client niet mag associëren.

Opmerking: wanneer een WLAN-clienttelling gelijk is aan nul, beëindigt de H-REAP alle gekoppelde 802.11 functies en niet langer taken voor de gegeven SSID. Dit beweegt de WLAN naar de volgende H-REAP status, **verificatie naar beneden, switching naar beneden**.

[Lokale verificatie, lokale switching](#)

In deze staat verwerkt het H-REAP LAP client-authenticaties en switches client-gegevenspakketten lokaal. Deze staat is alleen geldig in standalone-modus en alleen voor verificatietypen die lokaal kunnen worden verwerkt in het AP en waarbij geen verwerking van controller nodig is

De H-REAP die eerder in de **centrale authenticatie** was, **lokale switchstatus**, beweegt in deze staat, op voorwaarde dat het gevormde authenticatietype lokaal bij AP kan worden verwerkt. Als de geconfigureerde verificatie niet lokaal kan worden verwerkt, zoals 802.1x-verificatie, dan gaat de H-REAP in de standalone-modus naar **minder verificatie, lokale switching**-modus.

Dit zijn een aantal van de populaire authenticatiemechanismen die lokaal kunnen worden verwerkt op AP in standalone modus:

- Open (Openstaand)
- Gedeeld
- WAP-PSK
- WAP2-PSK

Opmerking: Alle echtheidsprocessen worden door de WLC verwerkt wanneer de AP in de aangesloten modus staat. Terwijl de H-REAP in standalone wijze is, worden de open, gedeelde, en de authenticatie van WAP/WAP2-PSK overgebracht naar de LAPs waar alle client authenticatie voorkomt.

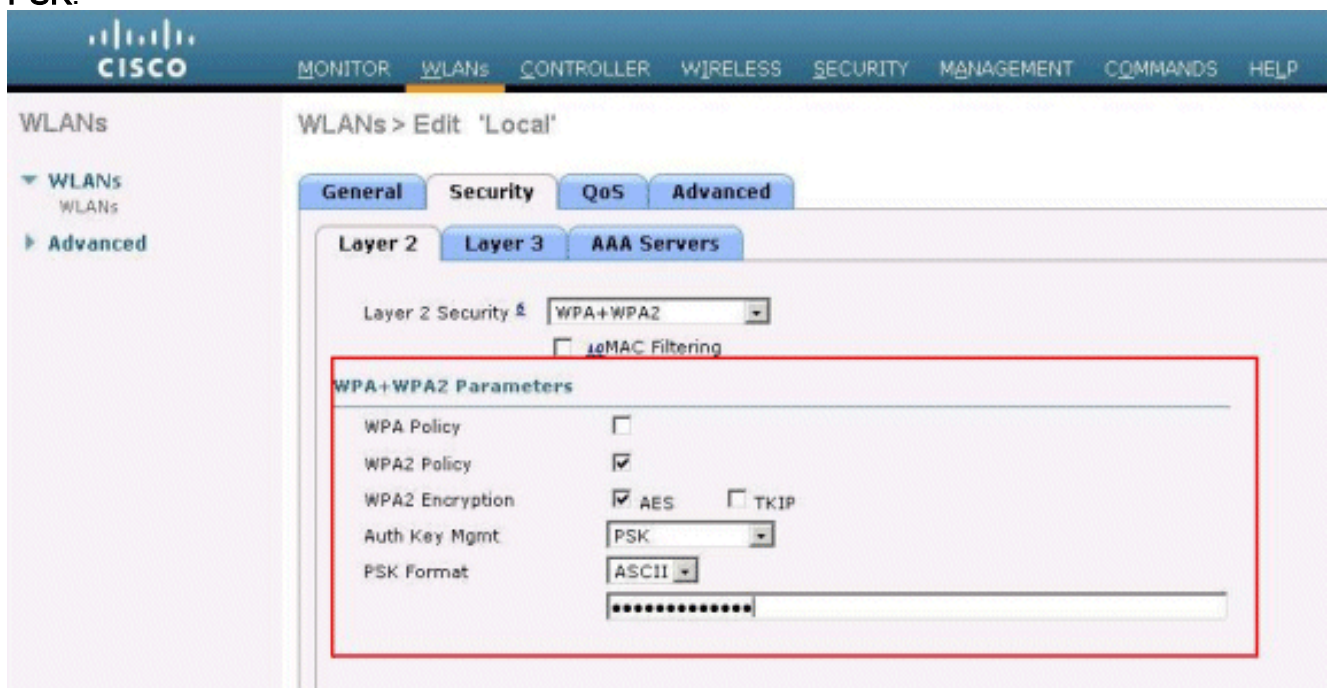
Opmerking: Externe webverificatie wordt niet ondersteund bij gebruik van hybride-REAP met lokale switching ingeschakeld op WLAN.

Dit voorbeeld gebruikt deze configuratie instellingen:

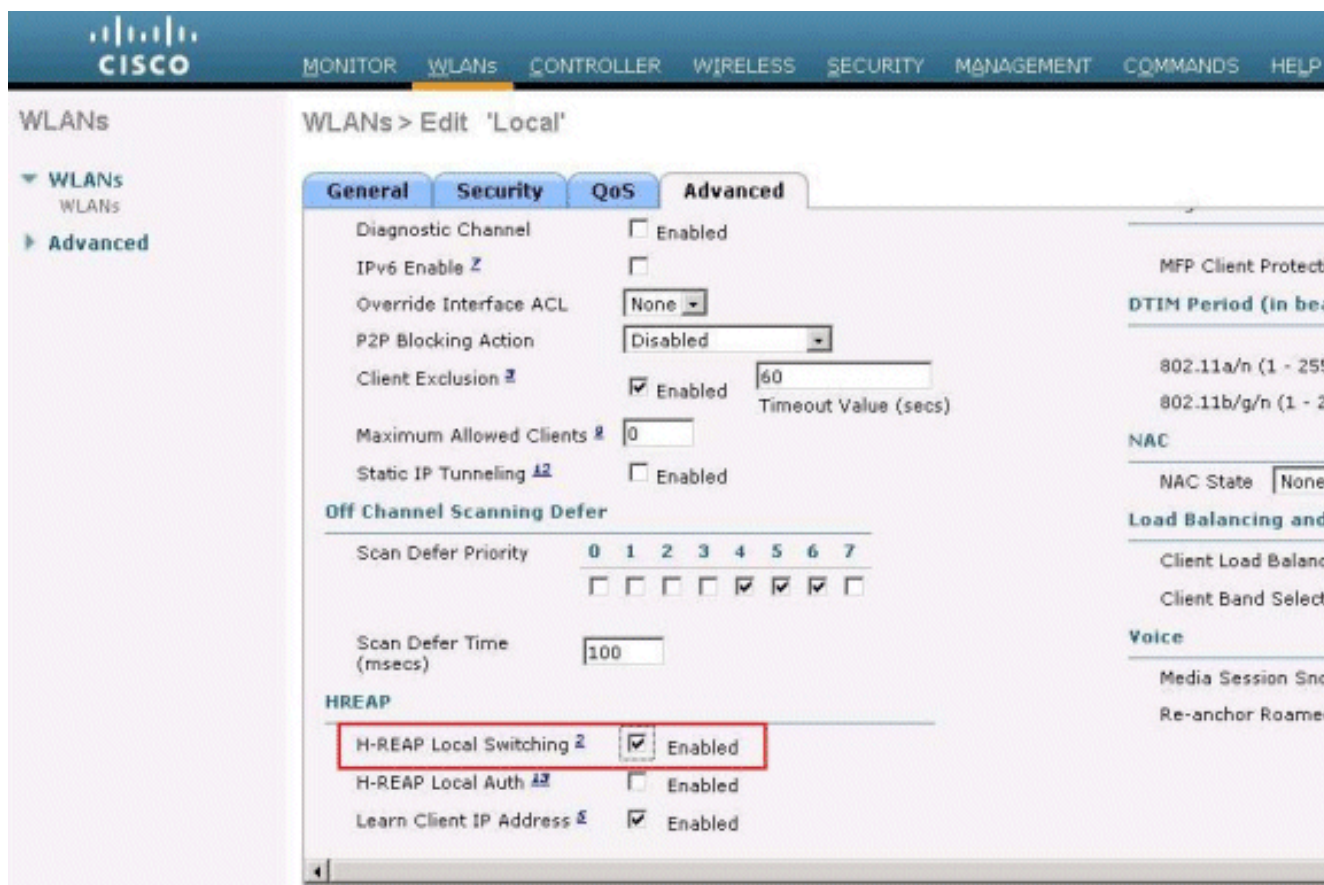
- WLAN/SSID-naam: **Lokaal**
- Layer 2 security: **WAP-PSK**
- Lokale switching: **H-REAP ingeschakeld**

Voltooi de volgende stappen vanuit de GUI-controller:

1. Klik op **WLAN's** om een nieuwe WLAN met de naam Local Area te maken en klik vervolgens op **Toepassen**.
2. Omdat dit WLAN lokale verificatie gebruikt, kiest u **WAP-PSK** of een van de bovengenoemde beveiligingsmechanismen die lokaal kunnen worden verwerkt in het veld Layer 2 security. Dit voorbeeld gebruikt **WAP-PSK**.



3. Indien geselecteerd, dient u de vooraf gedeelde sleutel/Pass Phrase te gebruiken. Dit moet aan de kant van de cliënt hetzelfde zijn om authenticatie succesvol te maken.
4. Controleer het aanvinkvakje **H-REAP Local Switching** om het clientverkeer te switches dat lokaal bij de H-REAP aan dit WLAN behoort.



Controleer lokale verificatie, lokale switching

Voer de volgende stappen uit:

1. Configureer de client met dezelfde SSID en beveiligingsconfiguraties. Hier is SSID *plaatselijk* en de veiligheidsmethode is *WAP-PSK*.
2. Activeert de lokale SSID in de client. De client wordt geauthentiseerd op de controller en associeert met de H-REAP. Het clientverkeer is lokaal ingesteld op switch. Nu is de H-REAP in Centrale Verificatie, Lokale Switching staat.
3. Schakel de WAN-link uit die op de controller wordt aangesloten. De verantwoordelijke zoals gewoonlijk gaat door het deregistratieproces. H-REAP is gedereguleerd door de controller. Als de H-REAP eenmaal is gedereguleerd, gaat hij over op een zelfstandige modus. Echter, de client die aan dit WLAN toebehoort, onderhoudt nog steeds associatie met H-REAP. Ook, omdat het authenticatietype hier lokaal kan worden verwerkt op de AP zonder de controller, staat H-REAP verenigingen van elke nieuwe draadloze client via deze WLAN toe.
4. Om dit te verifiëren, activeer elke andere draadloze client op dezelfde WLAN. U kunt zien dat de client geauthentiseerd en geassocieerd met succes is.

Problemen oplossen

- Als u problemen met de clientconnectiviteit wilt oplossen bij de poort van de H-REAP-console, voert u deze opdracht in:

```
AP_CLI#show capwap reap association
```
- Om problemen met de clientconnectiviteit bij de controller verder op te lossen en de uitvoer

van verdere debugging te beperken, gebruikt u deze opdracht:

```
AP_CLI#debug mac addr
```

- Om de 802.11 aansluitingsproblemen van een cliënt te zuiveren, gebruik deze opdracht:

```
AP_CLI#debug dot11 state enable
```

- Debug de 802.1X-verificatieprocedure van een client en fouten met deze opdracht:

```
AP_CLI#debug dot1x events enable
```

- Backend Controller/RADIUS-berichten kunnen met deze opdracht worden beveiligd:

```
AP_CLI#debug aaa events enable
```

- U kunt ook deze opdracht gebruiken om een compleet proces van client-**debug**-opdrachten in te schakelen:

```
AP_CLI#debug client
```

Gerelateerde informatie

- [Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point](#)
- [Configuratievoorbeeld van VLAN's voor draadloze LAN-controllers](#)
- [Configuratie-gids voor Cisco draadloze LAN-controllers, release 7.0](#)
- [Hybride REAP-ontwerp- en implementatiegids](#)
- [Hybride Remote Edge access point \(H-REAP\) - fundamentele probleemoplossing](#)
- [WLAN-controller-failover voor lichtgewicht access points - Configuratievoorbeeld](#)
- [Ondersteuning voor wireless producten](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)