

Aironet 600 Series access point voor buitengebruik configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Richtlijnen voor installatie](#)

[Overzicht van Office-uitbreidingsoplossing](#)

[Richtlijnen voor firewallconfiguratie](#)

[Configuratiestappen voor Office Extension AP-600](#)

[Configuratie-instellingen van WLAN en Remote LAN](#)

[WLAN-beveiligingsinstellingen](#)

[MAC-filtering](#)

[Ondersteunde gebruikers aantallen](#)

[Kanaalbeheer en -instellingen](#)

[Aanvullende voorbehouden](#)

[Configuratie van EAP-600 access point](#)

[OEAP-600 access point hardware-installatie](#)

[Probleemoplossing voor APEE-600](#)

[Hoe te debug client associatie problemen](#)

[Hoe het gebeurtenissenlogboek te interpreteren](#)

[Wanneer de internetverbinding onbetrouwbaar lijkt](#)

[Aanvullende debug-opdrachten](#)

[Bekende problemen/voorbehoud](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document bevat informatie over de vereisten voor het configureren van een Cisco Wireless LAN (WLAN)-controller voor gebruik met Cisco Aironet[®] 600 Series Office Extended Access Point (OEAP). Cisco Aironet 600 Series OEAP ondersteunt de werking in de gesplitste modus en heeft faciliteiten die configuratie via de WLAN-controller vereisen en functies die lokaal door de eindgebruiker kunnen worden geconfigureerd. Dit document bevat ook informatie over de configuraties die nodig zijn voor een goede verbinding en de ondersteunde functiesets.

[Voorwaarden](#)

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Aironet 600 Series Office Extended Access Point (OEAP).

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

Richtlijnen voor installatie

- Cisco Aironet 600 Series APEE wordt ondersteund op deze controllers: Cisco 5508, WiSM-2 en Cisco 2504.
- De eerste controllerrelease die Cisco Aironet 600 Series OEAP ondersteunt, is 7.0.16.0
- De beheerinterfaces van de controller moeten zich op een routeerbaar IP-netwerk bevinden.
- De configuratie van de bedrijfsfirewall moet worden gewijzigd om verkeer met UDP-poortnummers **5246** en **5247** mogelijk te maken.

Overzicht van Office-uitbreidingsoplossing

- Een gebruiker krijgt een toegangspunt met het IP-adres van de bedrijfscontroller, of de gebruiker kan het IP-adres van de controller invoeren via het configuratiescherm (HTML-pagina's instellen).
- De gebruiker steekt AP aan hun huisrouter.
- De AP krijgt een IP-adres van hun thuisrouter, sluit zich aan bij de vooraf ingestelde controller en maakt een beveiligde tunnel.
- Cisco Aironet 600 Series APEE adverteert vervolgens de collectieve SSID, die dezelfde beveiligingsmethoden en -services via het WAN uitbreidt naar het huis van de gebruiker.
- Als het externe LAN is geconfigureerd, wordt één bekabelde poort op de AP opnieuw getunneld naar de controller.
- De gebruiker kan dan ook een lokale SSID voor persoonlijk gebruik inschakelen.

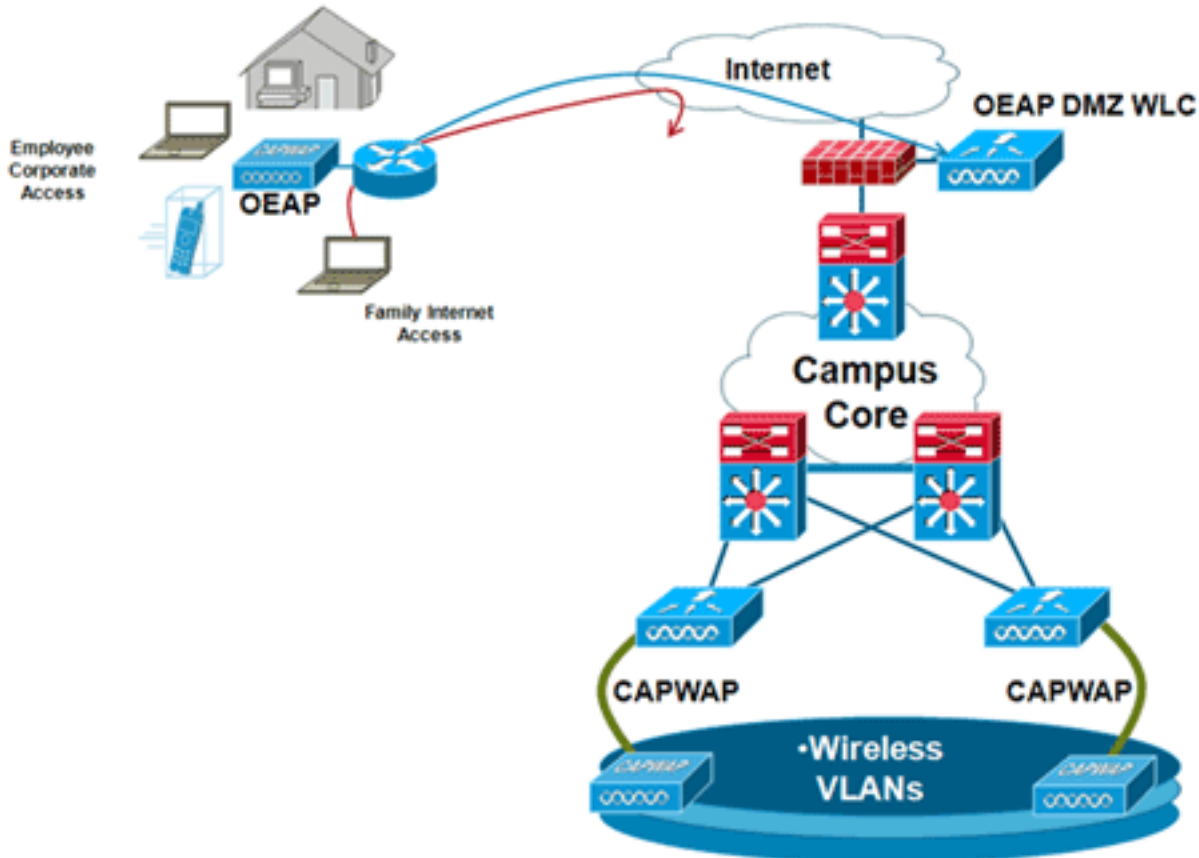
Richtlijnen voor firewallconfiguratie

De algemene configuratie op de firewall is om CAPWAP control en CAPWAP management

poortnummers door de firewall toe te staan. De Cisco Aironet 600 Series OEAP-controller kan in de DMZ-zone worden geplaatst.

Opmerking: de UDP 5246- en 5247-poorten moeten worden geopend op de firewall tussen de WLAN-controller en Cisco Aironet 600 Series POE.

Dit diagram toont een Cisco Aironet 600 Series OEAP-controller op de DMZ:



Hier is een voorbeeld van een firewallconfiguratie:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224
!--- X.X.X.X represents a public IP address ! interface Ethernet0/2 nameif dmz security-level 50
ip address 172.16.1.2 255.255.255.0 ! access-list Outside extended permit udp any host X.X.X.Y
eq 5246 !--- Public reachable IP of corporate controller access-list Outside extended permit udp
any host X.X.X.Y eq 5247 !--- Public reachable IP of corporate controller access-list Outside
extended permit icmp any any ! global (outside) 1 interface nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255 access-group Outside in
interface outside
```

Om het interne IP-adres van AP-Manager te verzenden naar OfficeExtend AP als onderdeel van het CAPWAPP Discovery Response-pakket, moet de controller-beheerder ervoor zorgen dat NAT is ingeschakeld in de AP-Manager-interface en dat het juiste NATed IP-adres naar het AP wordt verzonden.

Opmerking: standaard zal de WLC alleen reageren met het NAT IP-adres tijdens AP Discovery wanneer NAT is ingeschakeld. Als AP's binnen en buiten de NAT-gateway bestaan, geeft u deze opdracht uit om de WLC in te stellen om te reageren met zowel het NAT IP-adres als het niet-NAT (binnen) IP-adres voor beheer:

```
config network ap-discovery nat-ip-only disable
```

Opmerking: dit is alleen vereist als de WLC een NAT IP-adres heeft.

Dit diagram toont NAT is ingeschakeld, ervan uitgaande dat WLC een NAT IP-adres heeft:

The screenshot shows the Cisco WLC configuration interface for the 'management' interface. The 'NAT Address' section is highlighted with a red circle, indicating that NAT is enabled. The configuration details are as follows:

Section	Field	Value
General Information	Interface Name	management
	MAC Address	00:24:97:69:52:8f
Configuration	Quarantine	<input type="checkbox"/>
	Quarantine Vlan Id	0
NAT Address	Enable NAT Address	<input checked="" type="checkbox"/>
	NAT IP Address	X.X.X.Y
Interface Address	VLAN Identifier	0
	IP Address	172.16.1.25
	Netmask	255.255.255.0
	Gateway	172.16.1.2
Physical Information	The interface is attached to a LAG.	
	Enable Dynamic AP Management	<input checked="" type="checkbox"/>
DHCP Information	Primary DHCP Server	172.20.225.153
	Secondary DHCP Server	0.0.0.0

Opmerking: deze configuratie is niet vereist in de controller op voorwaarde dat deze is geconfigureerd met een routeerbaar IP-adres van internet en niet achter een firewall.

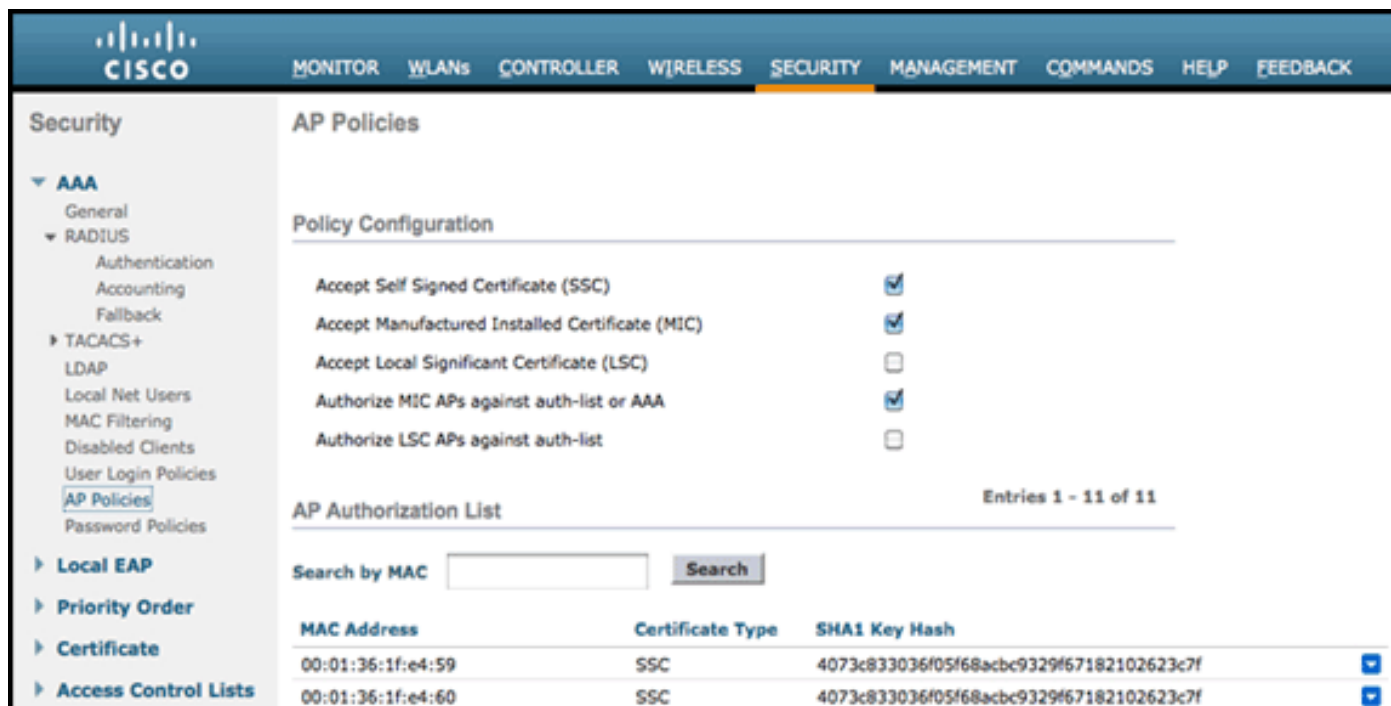
[Configuratiestappen voor Office Extension AP-600](#)

Cisco Aironet 600 Series access point zal op de WLC worden aangesloten als Local Mode access point.

Opmerking: de modi Monitor, H-REAP, Sniffer, Rogue Detection, Bridge en SE-Connect worden niet ondersteund op de 600-serie en zijn niet configureerbaar.

Opmerking: voor de functionaliteit van Cisco Aironet 600 Series OEAP in de 1040-, 1130-, 1140- en 3502i Series access points moet u de AP's voor hybride AP's (H-REAP) configureren en de submodus voor de AP instellen op Cisco Aironet 600 Series OEAP. Dit gebeurt niet met de 600 Series omdat de lokale modus wordt gebruikt en niet kan worden gewijzigd.

MAC-filtering kan worden gebruikt bij de verificatie van het toegangspunt tijdens het proces van eerste samenvoeging om te voorkomen dat onbevoegde Cisco Aironet 600 Series OEAP-eenheden zich bij de controller aansluiten. Dit beeld toont waar u het filteren van MAC toelaat en AP veiligheidsbeleid vormt:



The screenshot shows the Cisco Aironet 600 Series OEAP configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with options: AAA (General, RADIUS, Authentication, Accounting, Fallback, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies), Local EAP, Priority Order, Certificate, and Access Control Lists. The main content area is titled 'AP Policies' and 'Policy Configuration'. It lists several policy options with checkboxes: 'Accept Self Signed Certificate (SSC)' (checked), 'Accept Manufactured Installed Certificate (MIC)' (checked), 'Accept Local Significant Certificate (LSC)' (unchecked), 'Authorize MIC APs against auth-list or AAA' (checked), and 'Authorize LSC APs against auth-list' (unchecked). Below this is the 'AP Authorization List' section, which includes a search box for MAC addresses and a table with columns for MAC Address, Certificate Type, and SHA1 Key Hash. The table contains two entries for MAC address 00:01:36:1f:e4:59 and 00:01:36:1f:e4:60, both with Certificate Type SSC and SHA1 Key Hash 4073c833036f05f68acbc9329f67182102623c7f.

MAC Address	Certificate Type	SHA1 Key Hash
00:01:36:1f:e4:59	SSC	4073c833036f05f68acbc9329f67182102623c7f
00:01:36:1f:e4:60	SSC	4073c833036f05f68acbc9329f67182102623c7f

De Ethernet MAC (niet het Radio MAC-adres) wordt hier ingevoerd. Ook, als het invoeren van het MAC-adres in een Radius-server, moet een kleine case worden gebruikt. U kunt het AP Event-logbestand onderzoeken voor informatie over hoe u het Ethernet MAC-adres kunt ontdekken (meer hierover later).

[Configuratie-instellingen van WLAN en Remote LAN](#)

Er is één fysieke externe LAN-poort (gele #4) op Cisco Aironet 600 Series OEAP. Het is zeer gelijkaardig aan WLAN in hoe het wordt gevormd. Omdat het netwerk echter niet draadloos is en er een bekabelde LAN-poort aan de achterzijde van het toegangspunt is, wordt het toegangspunt uitgeroepen en beheerd als een externe LAN-poort.

Terwijl er slechts één fysieke poort op het apparaat is, kunnen maximaal vier bekabelde clients worden aangesloten als een hub of switch wordt gebruikt.

Opmerking: de limieten voor externe LAN-clients ondersteunen het aansluiten van een switch of hub op de externe LAN-poort voor meerdere apparaten of het rechtstreeks aansluiten op een Cisco IP-telefoon die is aangesloten op die poort.

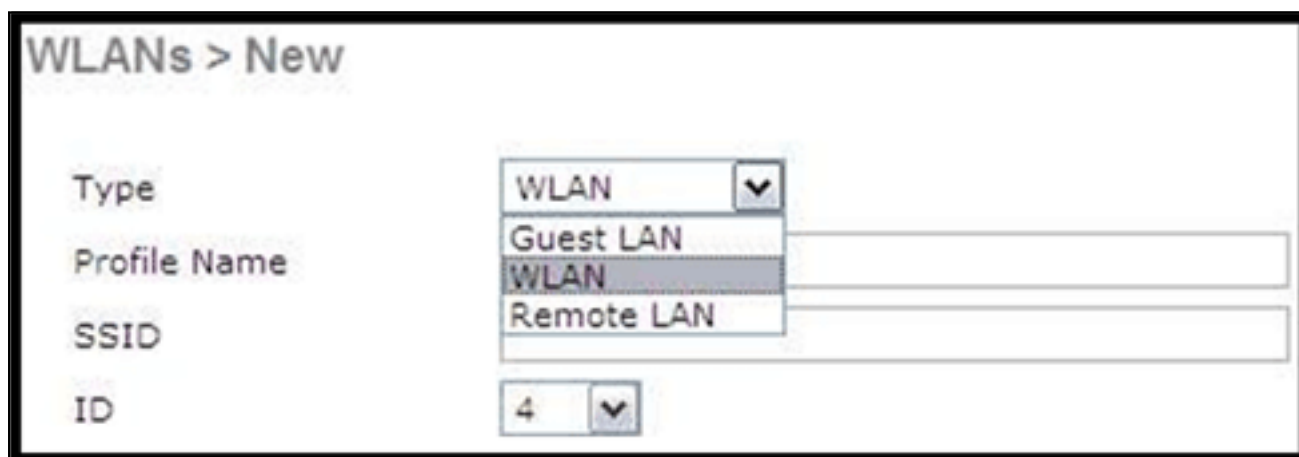
Opmerking: alleen de eerste vier apparaten kunnen verbinding maken totdat een van de apparaten langer dan een minuut inactief is. Als u 802.1x-verificatie gebruikt, kunnen er problemen zijn bij het gebruik van meer dan één client op de bekabelde poort.

Opmerking: dit nummer heeft geen invloed op de vijftien limiet die is opgelegd voor de controller WLAN's.

Een extern LAN wordt op dezelfde manier geconfigureerd als een WLAN en een gastLAN op de controller.

WLAN's zijn draadloze beveiligingsprofielen. Dit zijn de profielen die worden gebruikt door uw bedrijfsnetwerk. Cisco Aironet 600 Series OEAP ondersteunt ten hoogste twee WLAN's en één extern LAN.

Een extern LAN is vergelijkbaar met een WLAN, maar wordt toegewezen aan de bekabelde poort op de achterkant van het toegangspunt (#4 in geel) zoals in dit beeld:



N.B.: Als u meer dan twee WLAN's of meer dan één extern LAN hebt, moeten alle LAN's in een AP-groep worden geplaatst.

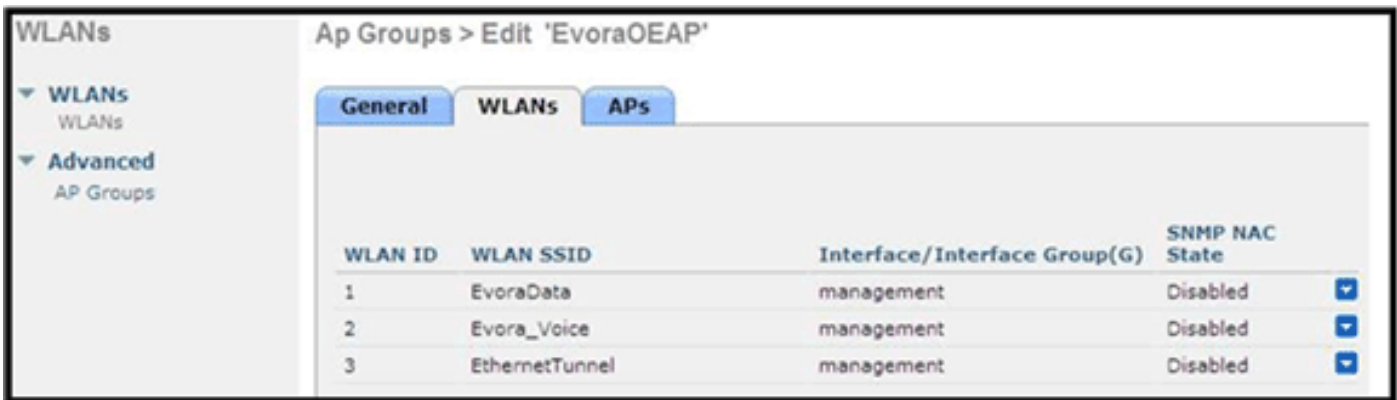
Dit beeld toont waar WLAN's en het externe LAN zijn geconfigureerd:



Deze afbeelding toont een voorbeeldnaam voor een EAP-groep:



Dit beeld toont een WLAN SSID- en RLAN-configuratie:

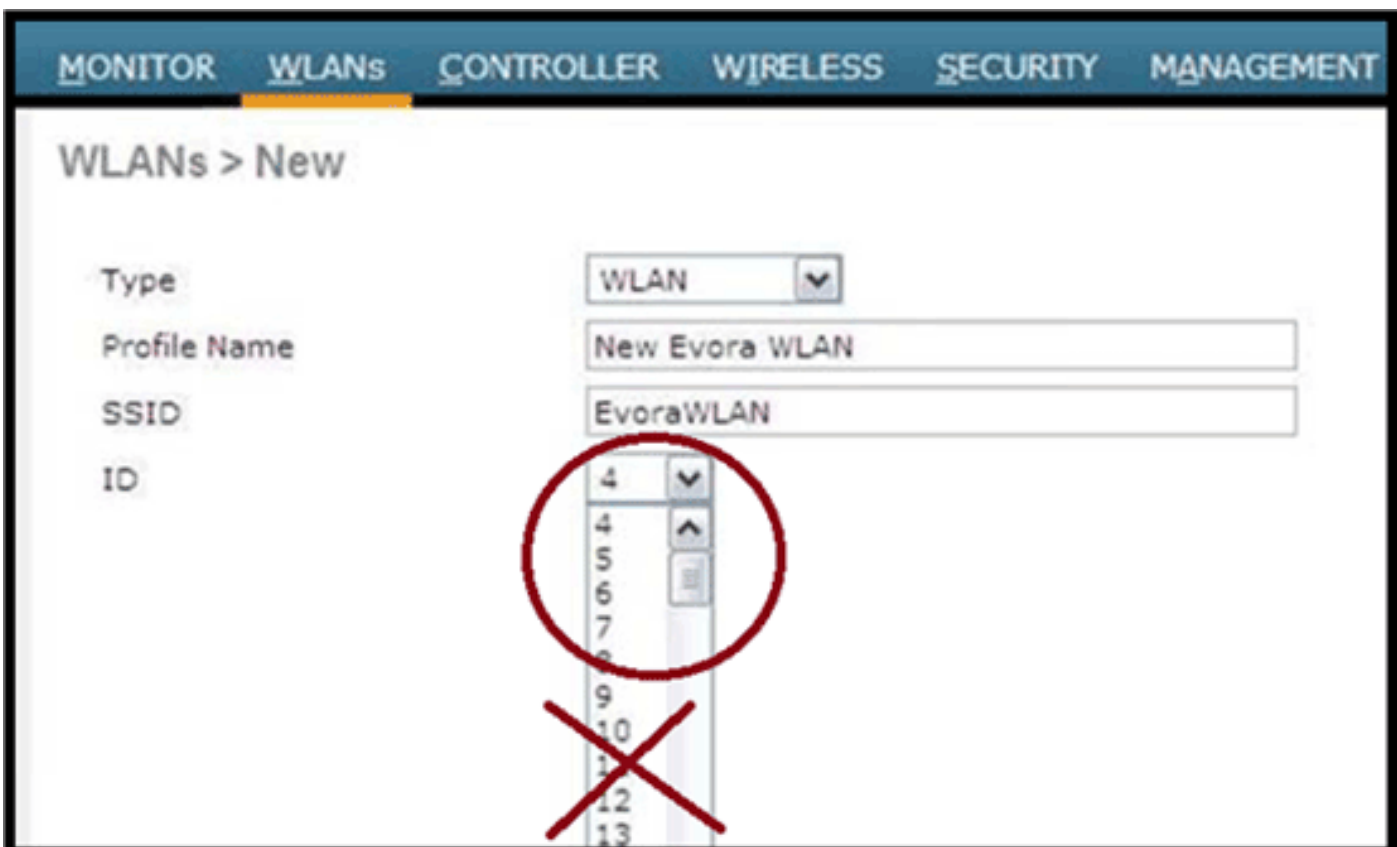


The screenshot shows the configuration page for an AP group named 'EvoraOEAP'. It features three tabs: 'General', 'WLANs', and 'APs'. The 'WLANs' tab is active, displaying a table with the following data:

WLAN ID	WLAN SSID	Interface/Interface Group(G)	SNMP NAC State
1	EvoraData	management	Disabled
2	Evora_Voice	management	Disabled
3	EthernetTunnel	management	Disabled

Als Cisco Aironet 600 Series EAP in een AP-groep is ingevoerd, zijn dezelfde limieten van twee WLAN's en één extern LAN van toepassing voor de configuratie van de AP-groep. Als Cisco Aironet 600 Series OEAP ook in de standaardgroep zit, wat betekent dat deze niet in een gedefinieerde AP-groep is, moeten de WLAN/externe LAN-id's worden ingesteld op minder dan ID 8, omdat dit product de hogere ID-groepen niet ondersteunt.

Bewaar ID-sets tot minder dan 8 zoals in deze afbeelding:



The screenshot shows the 'WLANs > New' configuration form. The 'Type' is set to 'WLAN'. The 'Profile Name' is 'New Evora WLAN' and the 'SSID' is 'EvoraWLAN'. The 'ID' field is a dropdown menu with values 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13. A red circle highlights the values 4, 5, 6, and 7, and a red 'X' is drawn over the values 8, 9, 10, 11, 12, and 13, indicating that IDs 8 and above are not supported.

Opmerking: Als extra WLAN's of externe LAN's worden gemaakt met de bedoeling de WLAN's of externe LAN's te wijzigen die door Cisco Aironet 600 Series OEAP worden gebruikt, schakelt u de huidige WLAN's of externe LAN's uit die u verwijdert voordat u de nieuwe WLAN's of externe LAN's op de 600 Series inschakelt. Als er meer dan één extern LAN is ingeschakeld voor een AP-groep, schakelt u alle externe LAN's uit en schakelt u vervolgens slechts één LAN in.

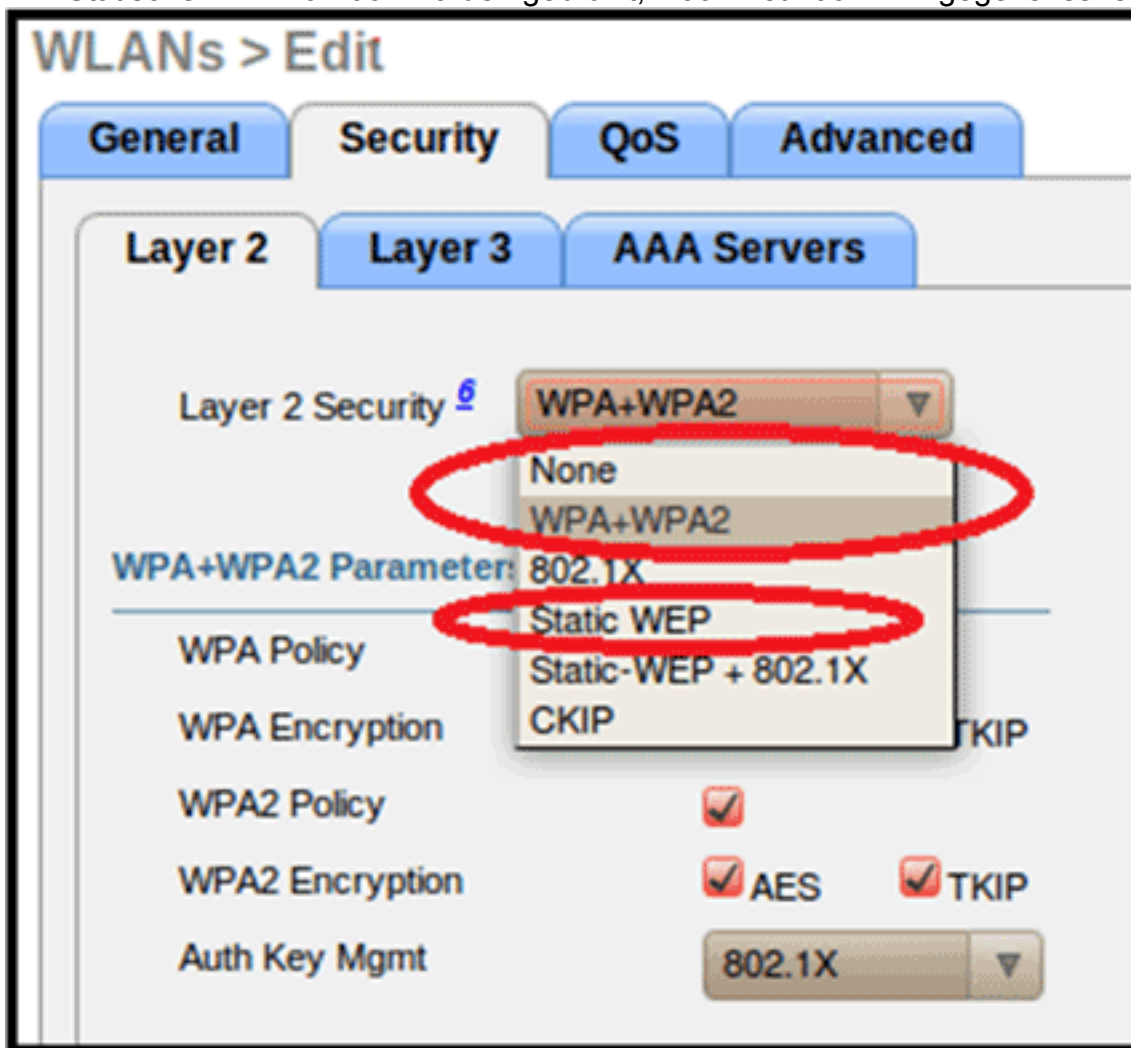
Als er meer dan twee WLAN's zijn ingeschakeld voor een AP-groep, schakelt u alle WLAN's uit en schakelt u vervolgens slechts twee WLAN's in.

WLAN-beveiligingsinstellingen

Wanneer u de beveiligingsinstelling in het WLAN instelt, zijn er specifieke elementen die niet worden ondersteund op de 600 Series.

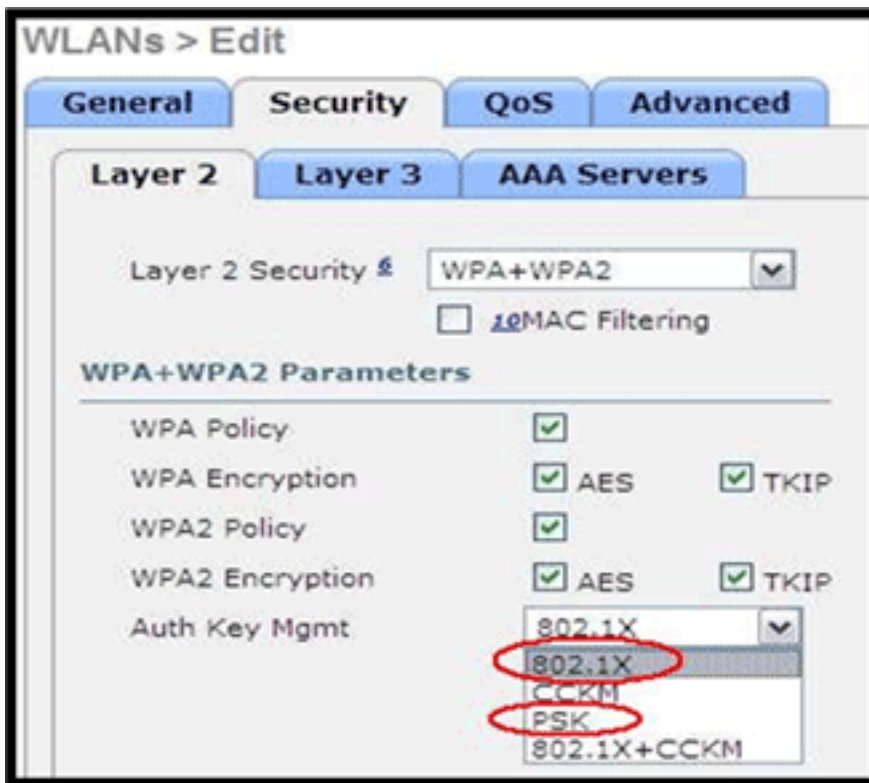
Voor Layer 2-beveiliging worden alleen deze opties ondersteund voor Cisco Aironet 600 Series OEAP:

- None
- WPA+WPA2
- Statische WEP kan ook worden gebruikt, maar niet voor .11n gegevensnelheden.

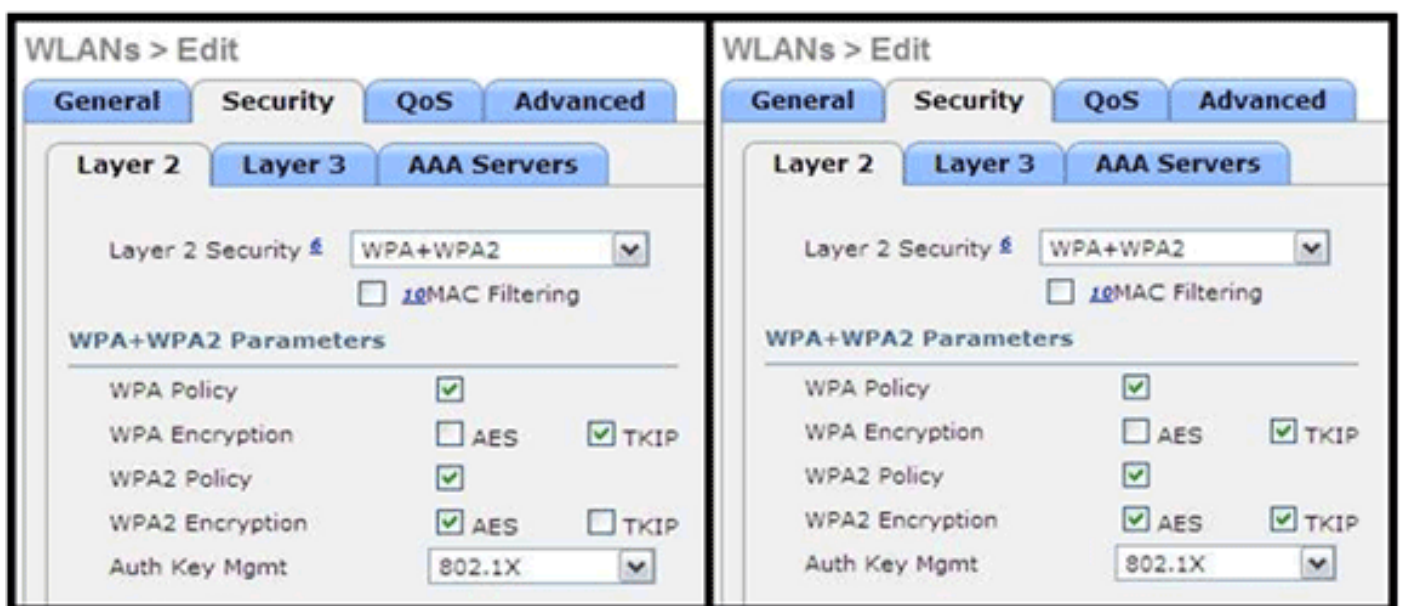


Opmerking: alleen 802.1x of PSK moet worden geselecteerd.

De instellingen voor de beveiligingscodering moeten identiek zijn voor WPA en WPA2 voor TKIP en AES, zoals in deze afbeelding wordt weergegeven:

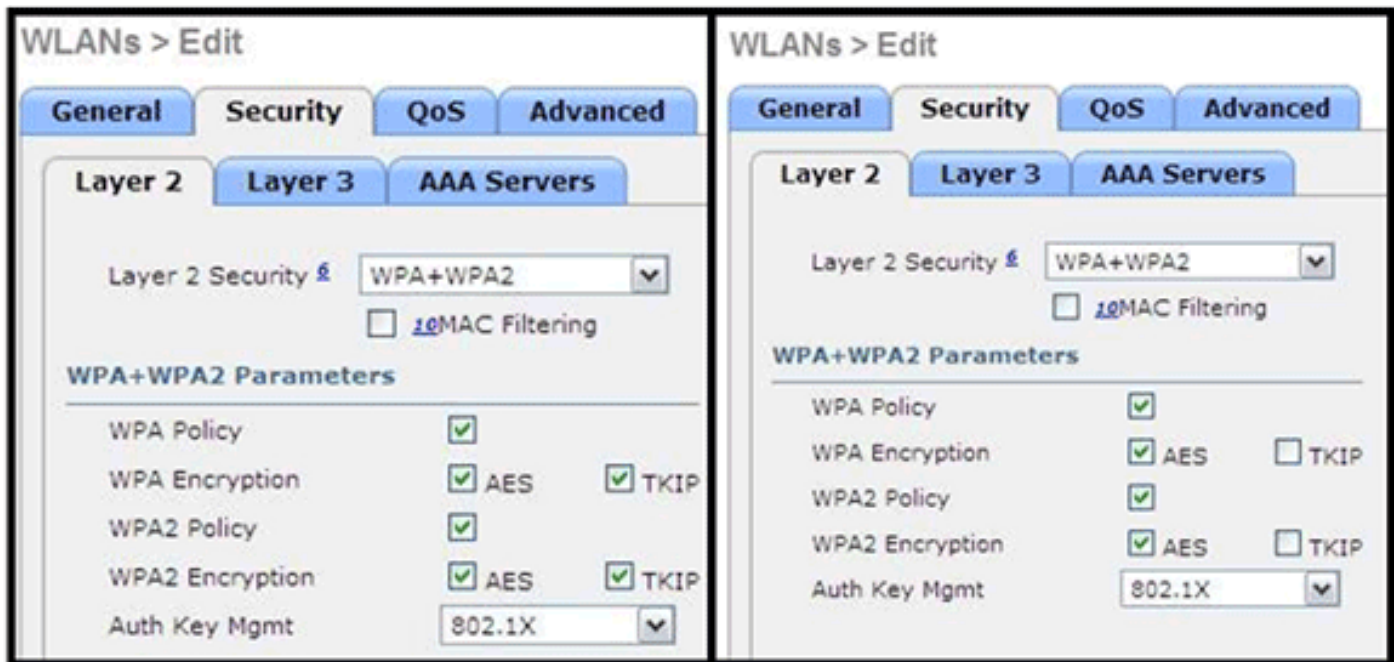


Deze afbeeldingen bevatten voorbeelden van incompatibele instellingen voor TKIP en AES:



Opmerking: houd er rekening mee dat beveiligingsinstellingen niet-ondersteunde functies mogelijk maken.

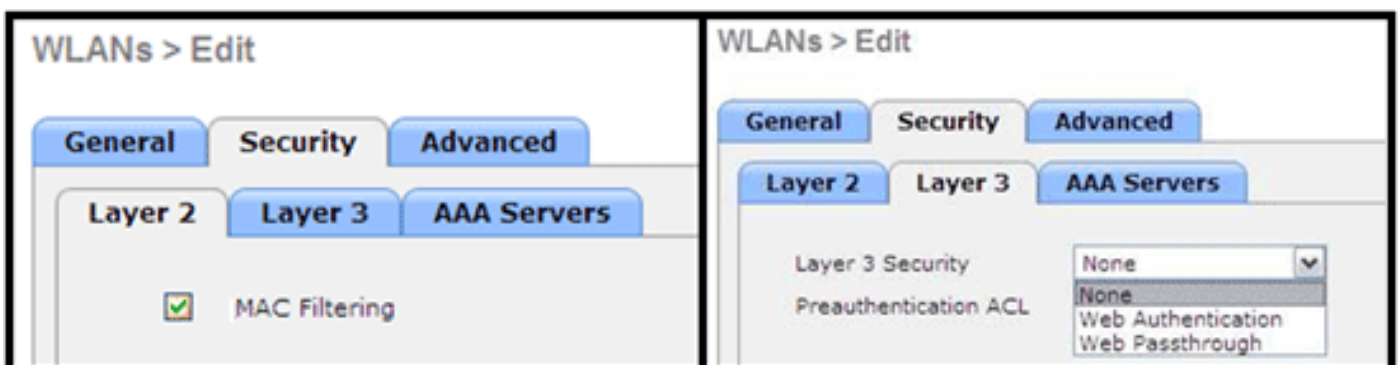
Deze afbeeldingen bevatten voorbeelden van compatibele instellingen:



MAC-filtering

Beveiligingsinstellingen kunnen worden opengelaten, ingesteld voor MAC-filtering of ingesteld voor Web Verification. Standaard wordt MAC-filtering gebruikt.

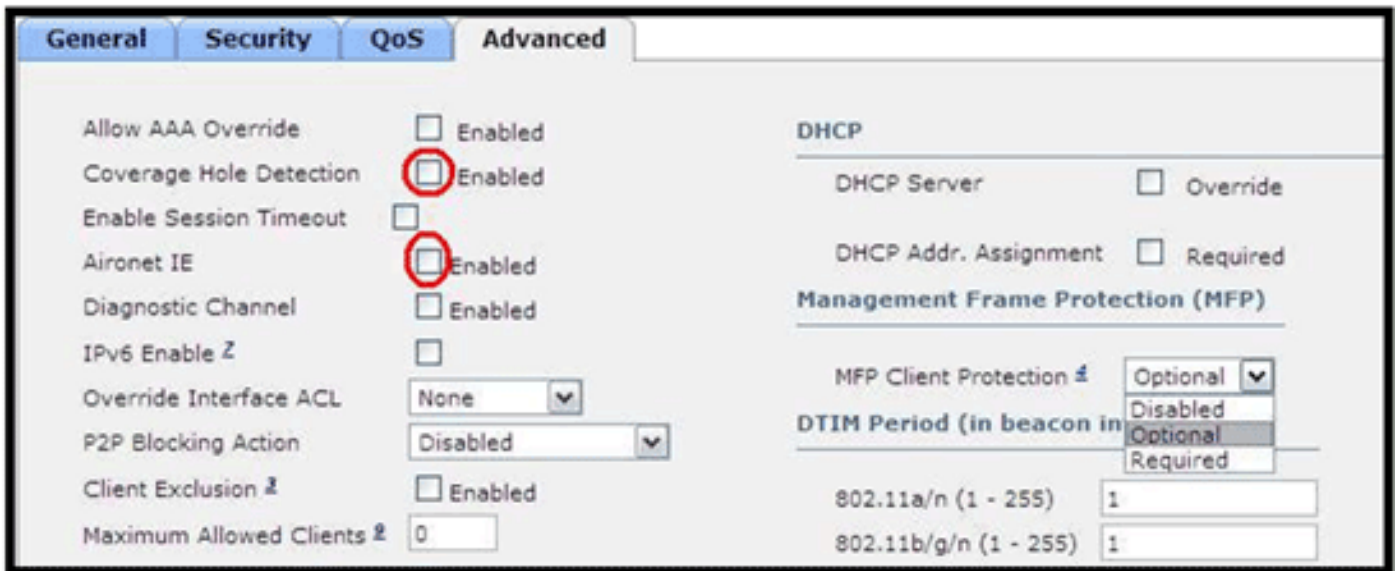
Dit beeld toont Layer 2 en Layer 3 MAC-filtering:



QoS-instellingen worden beheerd:

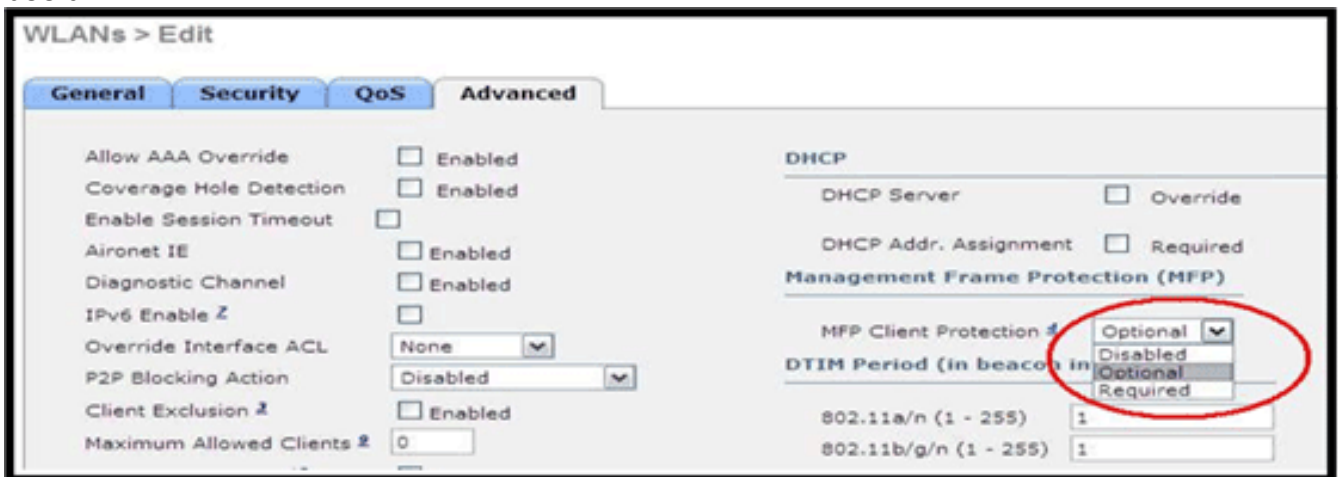


Geavanceerde instellingen moeten ook worden beheerd:

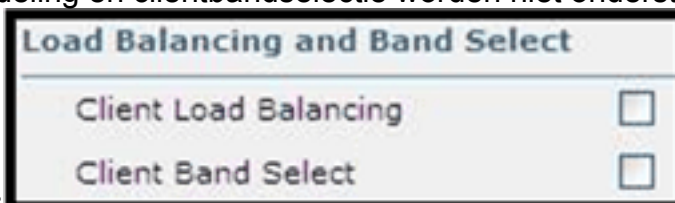


Opmerkingen:

- De detectie van klepgaten mag niet worden ingeschakeld.
- Aironet IE (Information Elements) mag niet worden ingeschakeld omdat deze niet worden gebruikt.
- Management Frame Protection (MFP) wordt ook niet ondersteund en moet als optioneel worden uitgeschakeld of geconfigureerd zoals in dit beeld:



- Clienttaakverdeling en clientbandselectie worden niet ondersteund en moeten niet worden



ingeschakeld:

Ondersteunde gebruikers aantallen

Slechts vijftien gebruikers mogen tegelijk verbinding maken met de WLAN-controller die op de 600-serie wordt geleverd. Een zestiende gebruiker kan niet authenticeren tot een van de eerste clients de-authenticates of een time-out heeft plaatsgevonden op de controller.

Opmerking: dit nummer is cumulatief voor de controller WLAN's van de 600-serie.

Als bijvoorbeeld twee controller WLAN's worden geconfigureerd en er vijftien gebruikers op een van de WLAN's zijn, kunnen geen gebruikers op dat moment verbinding maken met het andere WLAN op de 600-serie. Deze limiet is niet van toepassing op lokale privé WLAN's die de eindgebruiker op de 600 Series configureert voor persoonlijk gebruik en clients die op deze privé WLAN's of op de bekabelde poorten zijn aangesloten, hebben geen invloed op deze beperkingen.

Kanaalbeheer en -instellingen

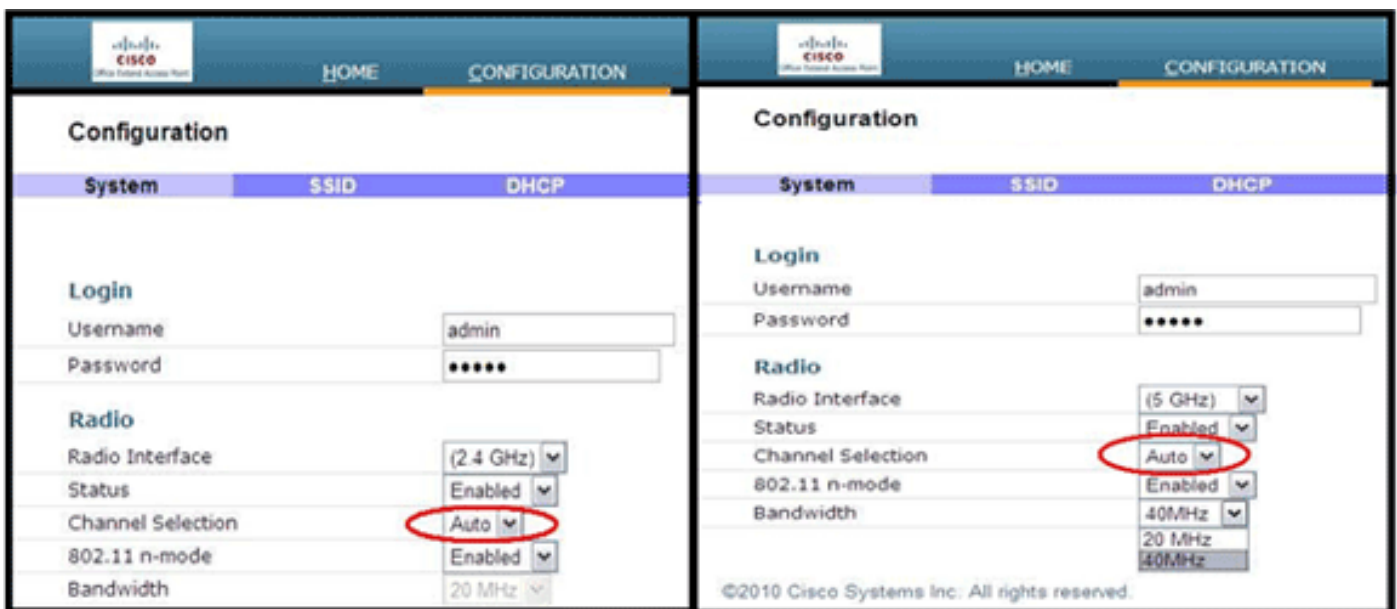
De radio's voor de 600-serie worden bestuurd via de lokale GUI op de 600-serie en niet via de draadloze LAN-controller.

Pogingen om het spectrumkanaal te controleren, de radio's aan te zetten of uit te schakelen via de controller zullen geen enkel effect hebben op de 600-serie.

De 600-serie scant en kiest kanalen voor 2,4 GHz en 5,0 GHz tijdens het opstarten, zolang de standaardinstellingen op de lokale GUI standaard blijven in beide spectra.

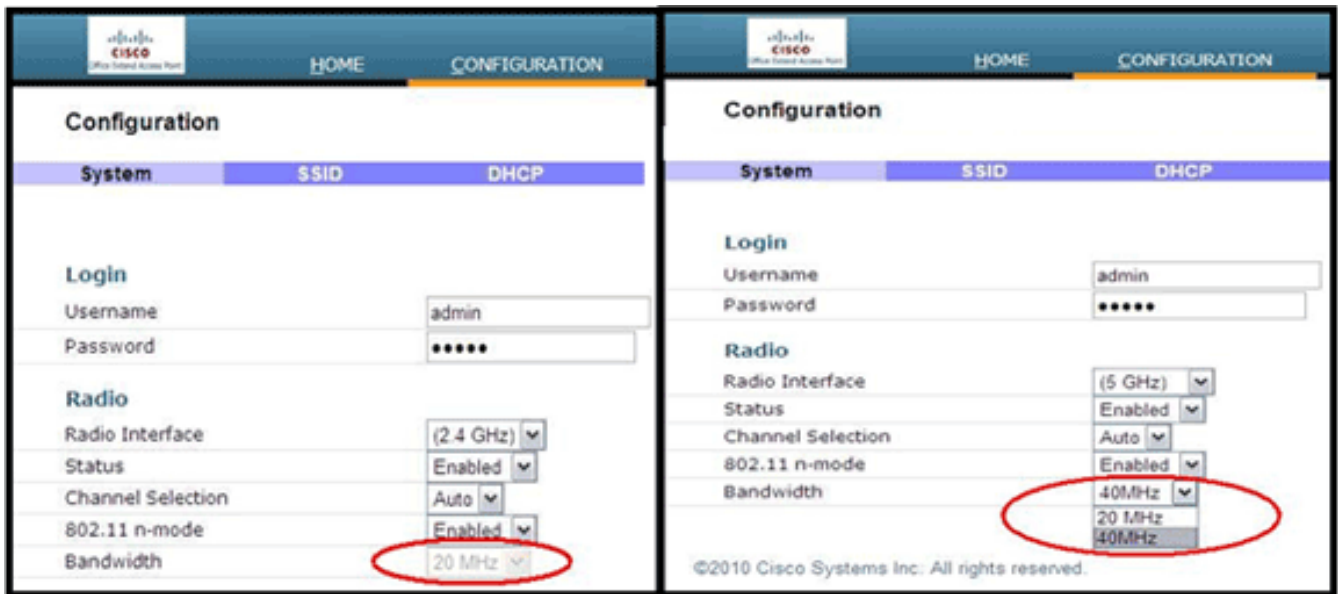
Opmerking: Als de gebruiker een of beide radio's lokaal uitschakelt (die radio is ook uitgeschakeld voor toegang door het bedrijf), ook zoals eerder vermeld, zijn RRM en geavanceerde functies zoals monitor, H-REAP, sniffer te veel voor de mogelijkheden van Cisco Aironet 600 Series OEAP die is geplaatst voor gebruik door thuisgebruikers en telewerkers.

De kanaalselectie en bandbreedte voor 5,0 GHz zijn hier geconfigureerd op de lokale GUI van Cisco Aironet 600 Series OEAP.



Opmerkingen:

- 20 en 40 MHz brede instellingen zijn beschikbaar voor 5 GHz.
- 2,4 GHz 40 MHz breed wordt niet ondersteund en is vast op 20 MHz.
- 40 MHz (channel bonding) wordt niet ondersteund in 2.4 GHz.

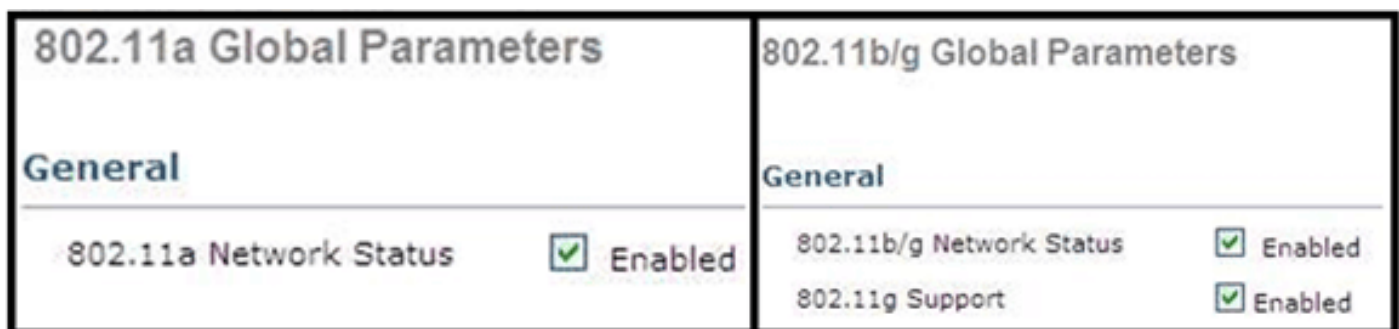


Aanvullende voorbehouden

Cisco Aironet 600 Series APEE is ontworpen voor single-AP implementaties. Daarom wordt client roaming tussen de 600-serie niet ondersteund.

Opmerking: als de 802.11a/n of 802.11b/g/n op de controller wordt uitgeschakeld, worden deze spectrums mogelijk niet uitgeschakeld op de Cisco Aironet 600 Series APEE omdat lokale SSID mogelijk nog steeds werkt.

De eindgebruiker heeft de controle over de radio's in/uit gezet binnen Cisco Aironet 600 Series OEAP.



Ondersteuning van 802.1x op de bekabelde poort

In deze eerste release wordt 802.1x alleen ondersteund op Command Line Interface (CLI).

Opmerking: GUI-ondersteuning is nog niet toegevoegd.

Dit is de bekabelde poort (#4 in geel) aan de achterzijde van Cisco Aironet 600 Series OEAP en is gekoppeld aan het externe LAN (zie vorige paragraaf over het configureren van extern LAN).

U kunt op ieder moment de **show**-opdracht gebruiken om de huidige externe LAN-configuratie weer te geven:

```
show remote-lan <remote-lan-id>
```

Om de externe LAN-configuratie te wijzigen, moet u deze eerst uitschakelen:

```
remote-lan disable <remote-lan-id>
```

802.1X-verificatie voor het externe LAN inschakelen:

```
config remote-lan security 802.1X enable <remote-lan-id>
```

U kunt deze opdracht ongedaan maken:

```
config remote-lan security 802.1X disable <remote-lan-id>
```

Voor het externe LAN is "Encryptie" altijd "Geen" (zoals wordt weergegeven in **show remote-lan**) en niet configureerbaar.

Als u lokale EAP (in de controller) wilt gebruiken als verificatieserver:

```
config remote-lan local-auth enable <profile-name> <remote-lan-id>
```

Waar het `profiel` is gedefinieerd via de controller-GUI (Security > Local EAP) of CLI (**configuratie Local-Audio**). Raadpleeg de controllerhandleiding voor meer informatie over deze opdracht.

U kunt dit ongedaan maken met deze opdracht:

```
config remote-lan local-auth disable <remote-lan-id>
```

Of, als u een externe AAA-verificatieserver gebruikt:

- **config remote-lan radius_server auth add/delete <remote-lan-id> <server-id>**
- **config remote-lan radius_server auth inschakelen/uitschakelen <remote-lan-id>**

Waar de `server` is geconfigureerd met de controller GUI (Security > RADIUS > Verificatie) of CLI (**config radius auth**). Raadpleeg de controllerhandleiding voor meer informatie over deze opdracht.

Nadat u klaar bent met de configuratie, schakelt u het externe LAN in:

```
config remote-lan enable <remote-lan-id>
```

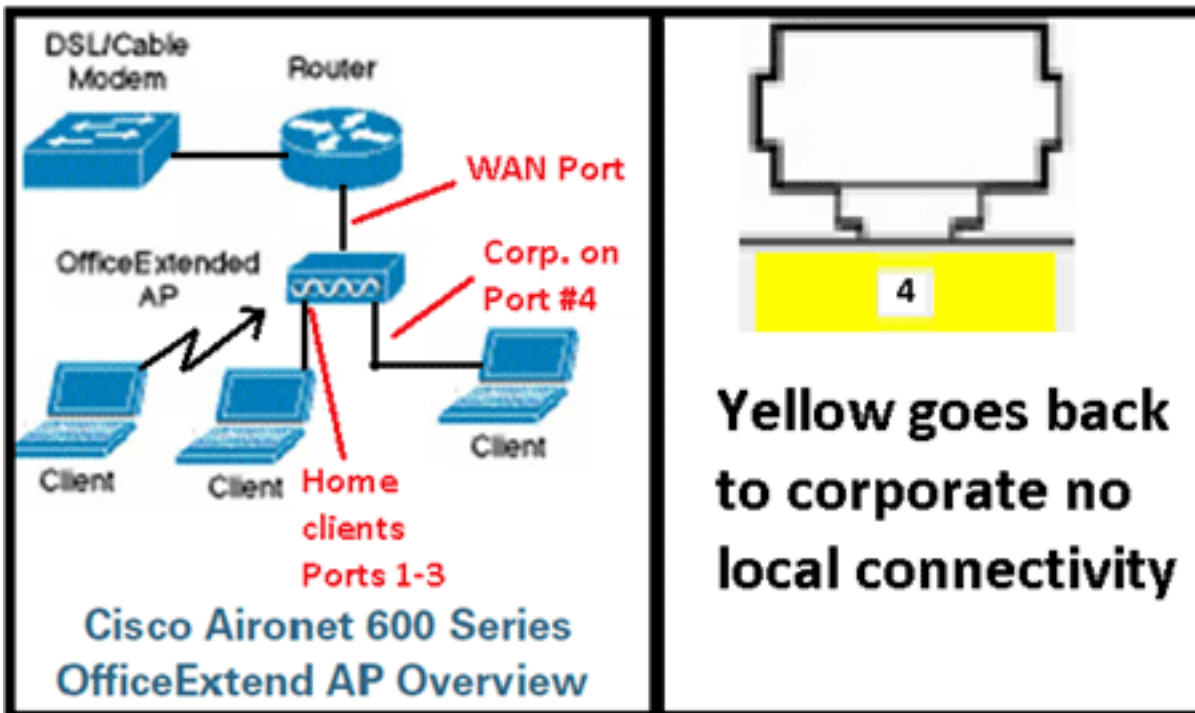
Gebruik de opdracht **show remote-lan <remote-lan-id>** om uw instelling te verifiëren.

Voor de externe LAN-client dient u 802.1X-verificatie in te schakelen en dienovereenkomstig te

configureren. Raadpleeg de gebruikershandleiding van het apparaat.

Configuratie van EAP-600 access point

Deze afbeelding toont het bedradingsdiagram voor Cisco Aironet 600 Series EAP:



Het standaard DHCP-bereik van Cisco Aironet 600 Series APEE is 10.0.0.x, zodat u naar het AP kunt bladeren op poorten 1-3 met behulp van het adres van 10.0.0.1. De standaardgebruikersnaam en het wachtwoord zijn beheerder.

N.B.: Dit is niet hetzelfde als de AP1040, 1130, 1140 en 3502i die Cisco als gebruikersnaam en wachtwoord hebben gebruikt.

Als de radio's omhoog zijn en een persoonlijke SSID reeds is gevormd, kunt u tot het configuratiescherm draadloos toegang hebben. Anders moet u lokale Ethernet-poorten 1-3 gebruiken.

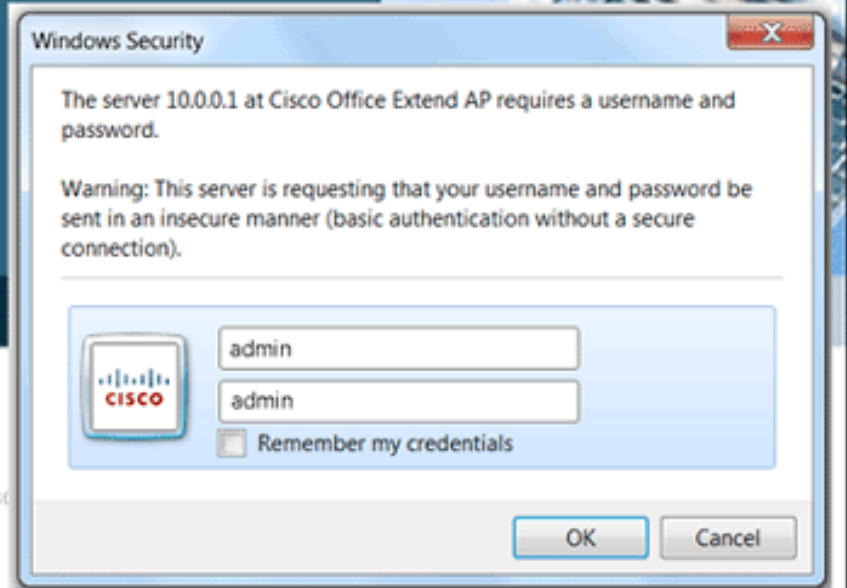
Om in te loggen, zijn de standaardgebruikersnaam en het wachtwoord admin.



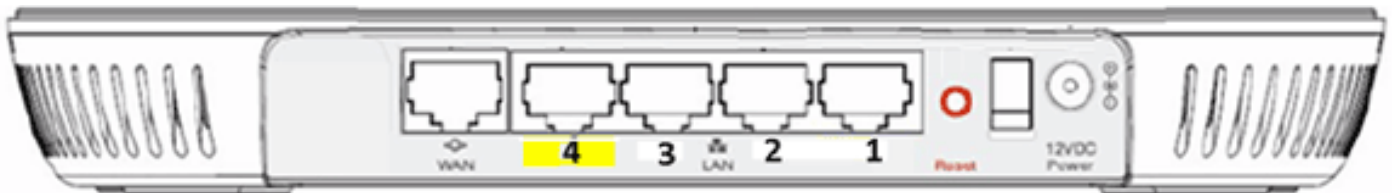
Office Extend Access Point

Enter

© 2005-2008 Cisco Systems
Cisco Systems, Inc. Cisco, Cisco Systems and Cisco
affiliates in the U.S. and other countries.



Opmerking: de gele #4 is niet actief voor lokaal gebruik. Als een extern LAN is geconfigureerd op de controller, wordt met deze poort opnieuw getunneld nadat het toegangspunt zich met succes bij de controller heeft aangesloten. Om naar het apparaat te bladeren, gebruikt u lokaal poorten 1-3:



Zodra u met succes naar het apparaat bladert, ziet u het scherm van de huisstatus. Dit scherm geeft radio- en MAC-statistieken. Als er geen radio's zijn geconfigureerd, kan de gebruiker in het configuratiescherm de radio's inschakelen, kanalen en modi instellen, lokale SSID's configureren en de WLAN-instellingen inschakelen.

Configuration Apply

System **SSID** **DHCP** **WAN**

Login

Username:

Password:

Radio

Radio Interface: ⓘ Select Each Radio and Configure Independently

Status:

Channel Selection:

802.11 n-mode: ⓘ 802.11n is not supported with TKIP-only WPA Encryption

Bandwidth:

Van het scherm SSID is waar de gebruiker het persoonlijke WLAN-netwerk kan configureren. De bedrijfsradio-SSID en de beveiligingsparameters worden ingesteld en van de controller afgedrukt (nadat u het WAN met de IP van de controller hebt geconfigureerd), en er is een geslaagde verbinding opgetreden.

Dit beeld toont een SSID lokale MAC filtering configuratie:

Configuration Apply

System **SSID** **DHCP** **WAN**

Personal Network

Band Selection: ⓘ Select Each Radio and Configure SSID Individually

Enabled:

Broadcast:

SSID: ⓘ Personal SSID should be different from Corporate SSID

MAC Filter

Enabled:

Allowed MAC Addresses:

Nadat de gebruiker de persoonlijke SSID configureren, staat het onderstaande scherm de gebruiker toe om de beveiliging op de private home SSID in te stellen, radio's in te schakelen en zo nodig MAC-filtering te configureren. Als het persoonlijke netwerk 802.11n-snelheden gebruikt, wordt de gebruiker aangeraden om een verificatietype, een coderingstype en een wachtwoord voor WPA2-PSK en AES te kiezen.

Opmerking: deze SSID-instellingen verschillen van de bedrijfsinstellingen als de gebruiker ervoor kiest om een of beide van de radio's uit te schakelen (beide zijn ook uitgeschakeld voor gebruik door het bedrijf).

Gebruikers die lokaal toegang hebben tot de beheerinstellingen hebben controle over kernfuncties zoals radio inschakelen/uitschakelen tenzij het apparaat is beveiligd met een wachtwoord en geconfigureerd door de beheerder. Daarom moet ervoor worden gezorgd dat beide radio's niet worden uitgeschakeld, aangezien dit kan leiden tot een verlies van connectiviteit, zelfs als het apparaat met succes toetreedt tot de controller.

Dit beeld toont de beveiligingsinstellingen van het systeem:



Security	
WPA-PSK	Disabled ▼
WPA2-PSK	Enabled ▼
WEP Encryption	Disabled ▼
WPA Encryption	AES ▼
WPA passphrase	••••• Click here to display
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	2 ▼

Verwacht wordt dat de thuiswerker de Cisco Aironet 600 Series APEE achter een thuisrouter installeert, aangezien dit product niet is ontworpen om de functionaliteit van een thuisrouter te vervangen. Dit komt doordat de huidige versie van dit product geen firewallondersteuning, PPPoE-ondersteuning of poortdoorsturen heeft. Dit zijn functies die klanten verwachten te vinden in een thuisrouter.

Terwijl dit product kan werken zonder een huisrouter, wordt het aanbevolen om het niet zo te plaatsen om de vermelde redenen. Ook kunnen er compatibiliteitsproblemen zijn die rechtstreeks verband houden met bepaalde modems.

Gezien het feit dat de meeste thuisrouters een DHCP-scope hebben in het 192.168.x.x bereik, heeft dit apparaat een standaard DHCP-scope van 10.0.0.x en is configureerbaar.

Als de thuisrouter 10.0.0.x gebruikt, moet u Cisco Aironet 600 Series OEAP configureren om een 192.168.1.x of compatibel IP-adres te gebruiken om netwerkconflicten te voorkomen.

Dit beeld toont een DHCP-toepassingsconfiguratie:

The screenshot shows the Cisco configuration interface. At the top, there is a navigation bar with 'HOME', 'CONFIGURATION', and 'EVENT_LOG'. Below this, the 'Configuration' section is active, with an 'Apply' button. A menu bar highlights 'System', 'SSID', 'DHCP', and 'WAN'. The 'Local DHCP' section contains the following settings:

System	SSID	DHCP	WAN
Local DHCP			
IP Address	10.0.0.1		
Subnet Mask	255.255.255.0		
Default Gateway	10.0.0.1		
DHCP Server	Enabled ▾		
DHCP Starting IP Address	10.0.0.100		
DHCP Ending IP Address	10.0.0.150		
DHCP Lease Time	86400		

Let op: als Cisco Aironet 600 Series APEE niet gefaseerd of geconfigureerd is door de IT-beheerder, moet de gebruiker het IP-adres van de bedrijfscontroller invoeren (zie hieronder) zodat het toegangspunt zich met succes bij de controller kan aansluiten. Na een succesvolle deelname moet het toegangspunt de nieuwste afbeelding van de controller en de configuratieparameters zoals de WLAN-instellingen van het bedrijf downloaden. Indien geconfigureerd ook de bekabelde poortinstellingen voor extern LAN aan de achterzijde van Cisco Aironet 600 Series #4.

Als het niet toetreedt, controleer dat het IP-adres van de controller via het internet bereikbaar is. Als MAC-filtering is ingeschakeld, controleert u of het MAC-adres met succes in de controller is ingevoerd.

Deze afbeelding toont het IP-adres van de Cisco Aironet 600 Series OEAP-controller:

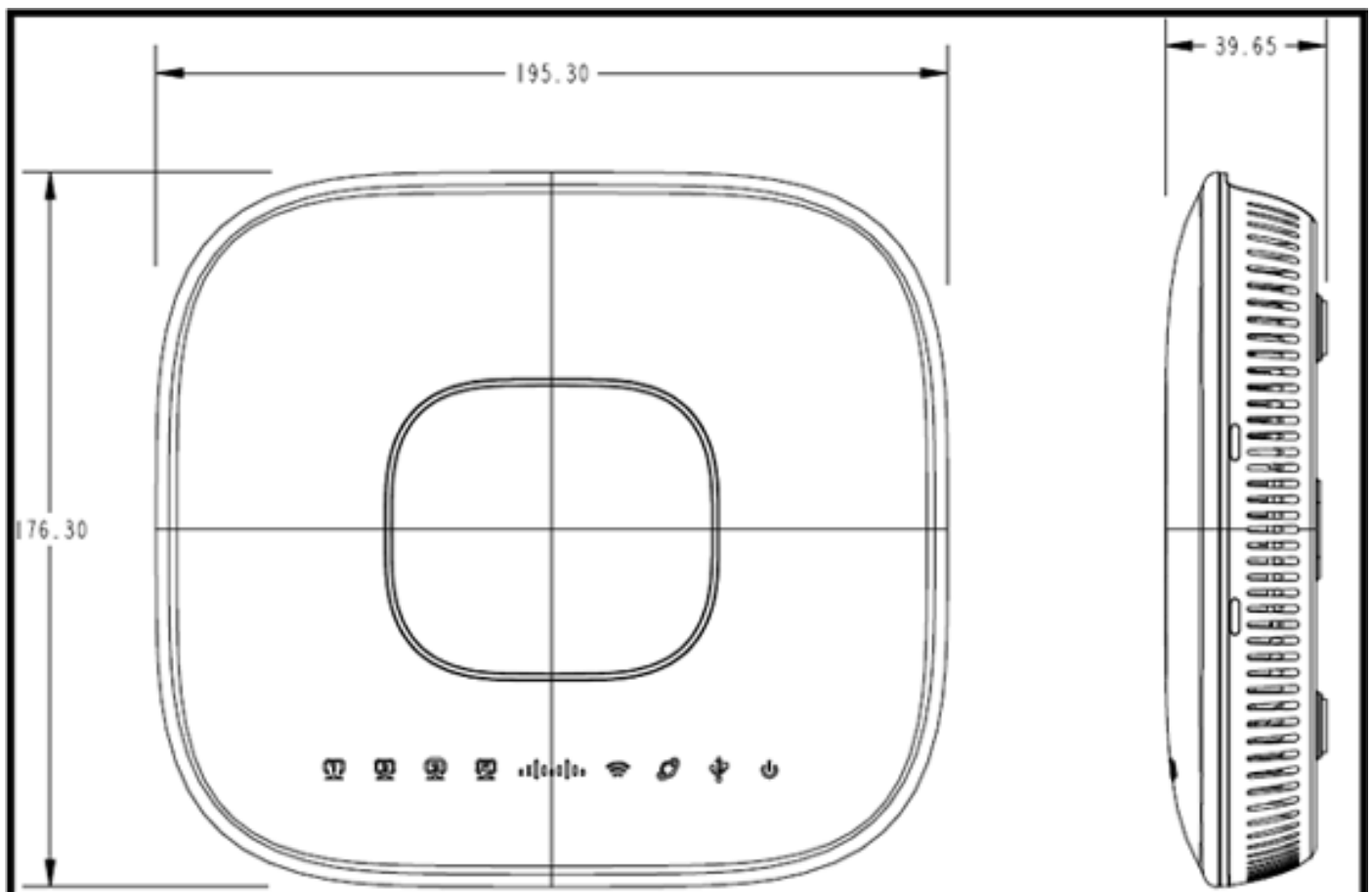
CISCO HOME CONFIGURATION EVENT_LOG

Configuration Apply

System	SSID	DHCP	WAN
This is where you enter the IP address of the DMZ OEAP controller			
Controller		IP Address <input type="text" value="Y.Y.Y.Y"/>	
Uplink IP Configuration		Example IP	
Static IP	<input type="checkbox"/>		
Domain Name	<input type="text" value="gateway.2wire.net"/>		
IP Address	<input type="text" value="192.168.1.68"/>		
Subnet Mask:	<input type="text" value="255.255.255.0"/>		
Default Gateway	<input type="text" value="192.168.1.254"/>		
DNS Server	<input type="text" value="192.168.1.254"/>		

[OEAP-600 access point hardware-installatie](#)

Deze afbeelding toont de fysieke aspecten van Cisco Aironet 600 Series APEE:

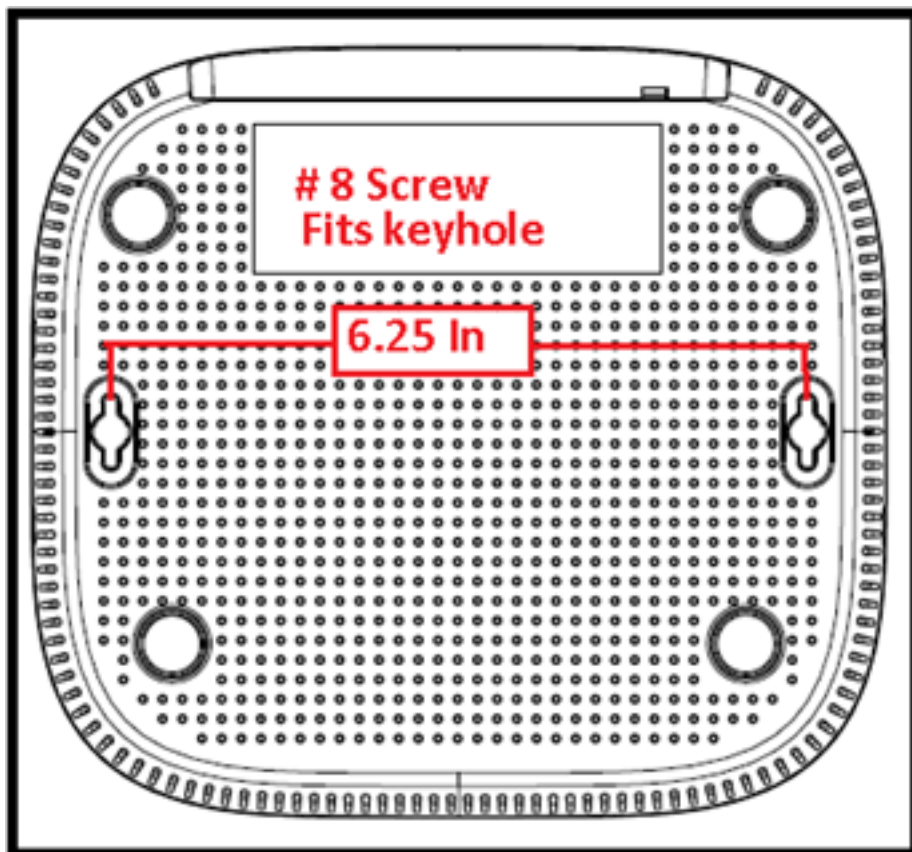


Dit toegangspunt is ontworpen om op een tafel te worden gemonteerd en heeft rubberen voetjes. Het kan ook wandmontage, of kan recht op zitten met behulp van de meegeleverde wieg. Probeer

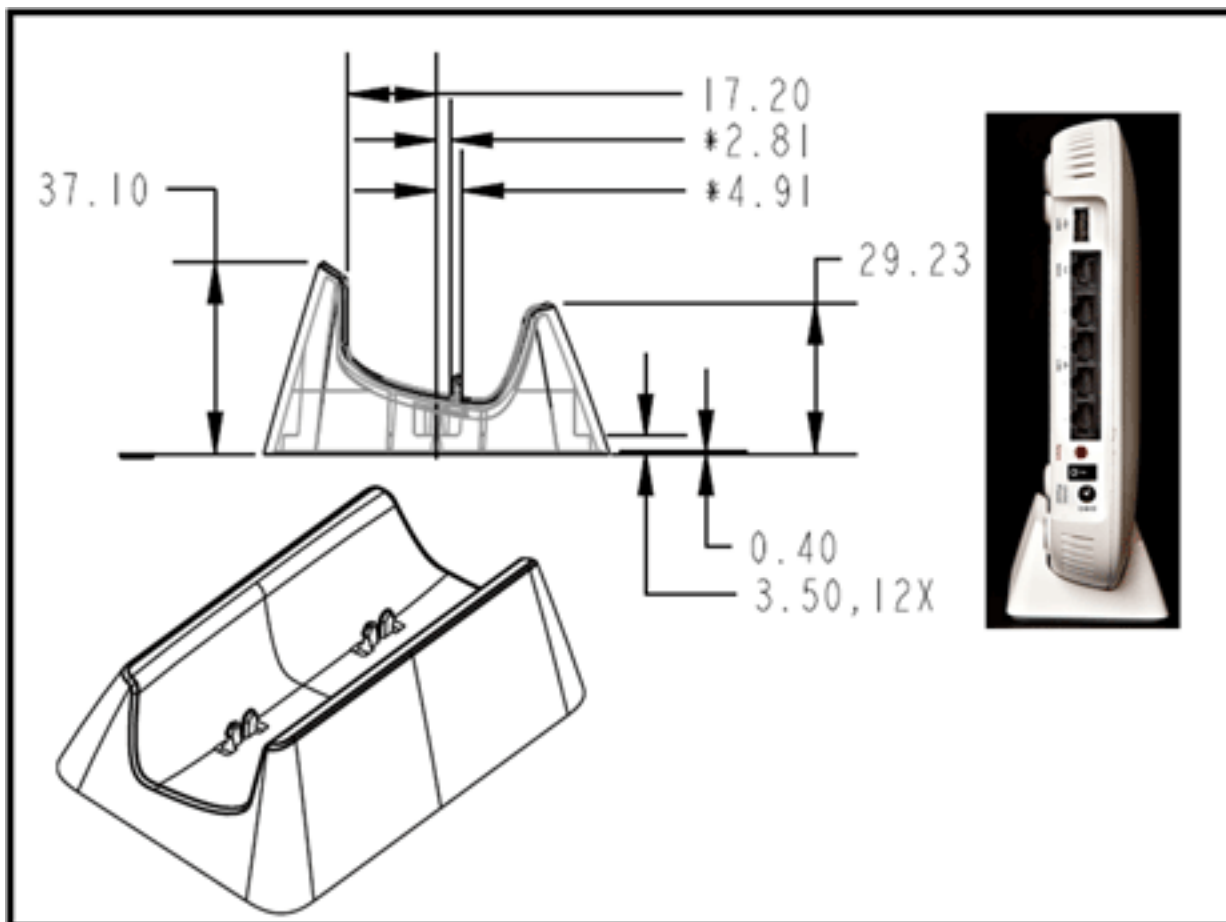
het toegangspunt zo dicht mogelijk bij de bedoelde gebruikers te plaatsen. Vermijd gebieden met grote metalen oppervlakken, zoals het plaatsen van het apparaat op een metalen bureau of in de buurt van een grote spiegel. De meer muren en objecten tussen het toegangspunt en de gebruiker zorgen voor een lager signaal en kunnen de prestaties verminderen.

Opmerking: dit toegangspunt gebruikt een voeding van +12 volt en maakt geen gebruik van Power over Ethernet (PoE). Het apparaat levert ook geen PoE. Zorg ervoor dat de juiste voedingsadapter wordt gebruikt in combinatie met het toegangspunt. Zorg er ook voor dat u geen andere adapters van andere apparaten gebruikt, zoals laptops en IP-telefoons, aangezien deze het toegangspunt kunnen beschadigen.

Het apparaat kan aan de muur worden bevestigd met plastic ankers of houtschroeven.



Het apparaat kan rechtop worden gemonteerd met behulp van de meegeleverde wieg.



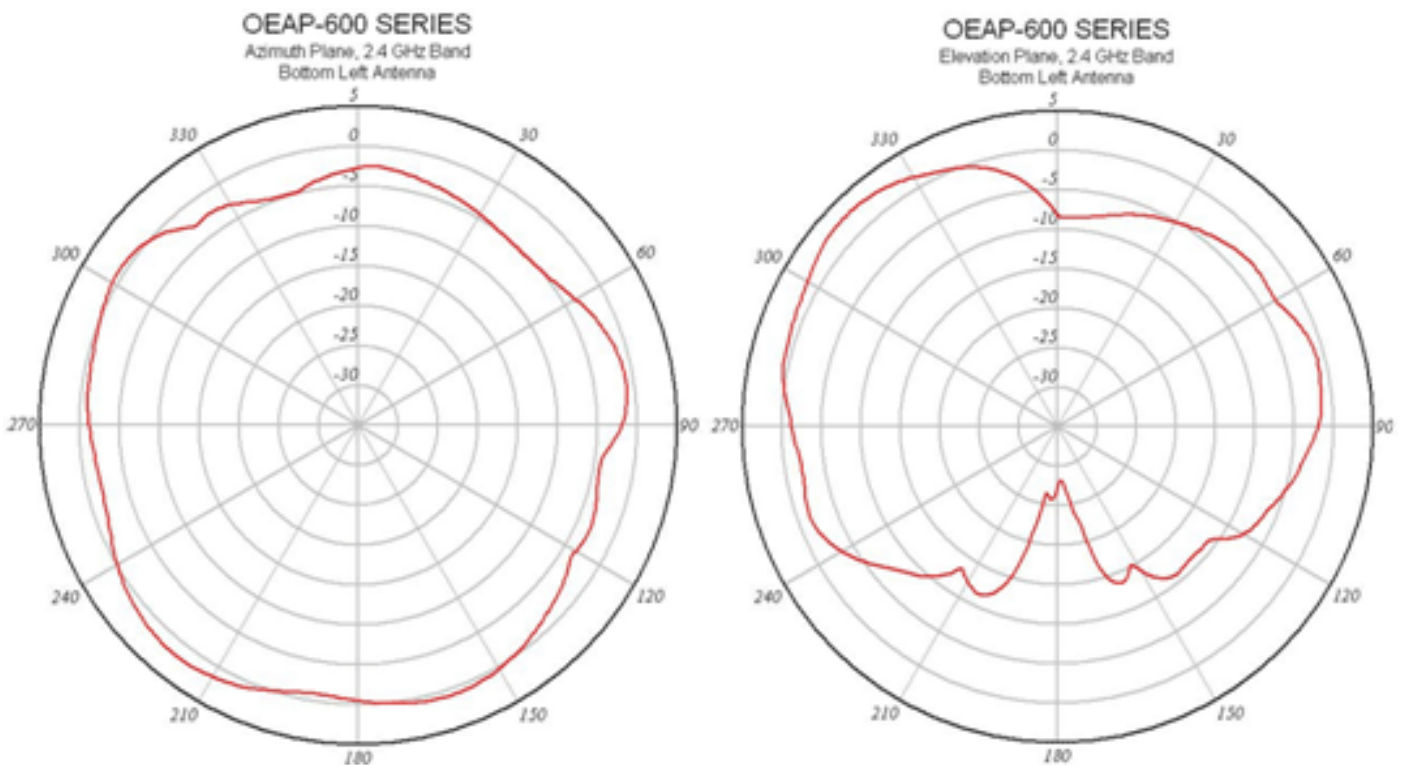
Cisco Aironet 600 Series APEE heeft antennes aan de randen van het toegangspunt. De gebruiker dient ervoor te zorgen dat het toegangspunt niet wordt geplaatst in de buurt van metalen objecten of obstakels waardoor het signaal kan afnemen of richten. De antenneversterking is ongeveer 2 dBi in beide banden en ontworpen om te stralen in een 360 graden patroon. Gelijkaardig aan een gloeilamp (zonder een lampschaduw), is het doel om in alle richtingen uit te stralen. Denk aan het toegangspunt zoals bij een lamp en probeer deze dicht bij de gebruikers te plaatsen.

Metalen objecten, zoals spiegels, belemmeren het signaal net zoals de lampenkap analogie. U kunt een verminderde doorvoersnelheid of bereik ervaren als het signaal moet doordringen of door vaste objecten moet gaan. Als u connectiviteit verwacht, bijvoorbeeld in een huis met drie verdiepingen, vermijd het plaatsen van de AP in de kelder en probeer om de AP op een centrale locatie binnen het huis te monteren.

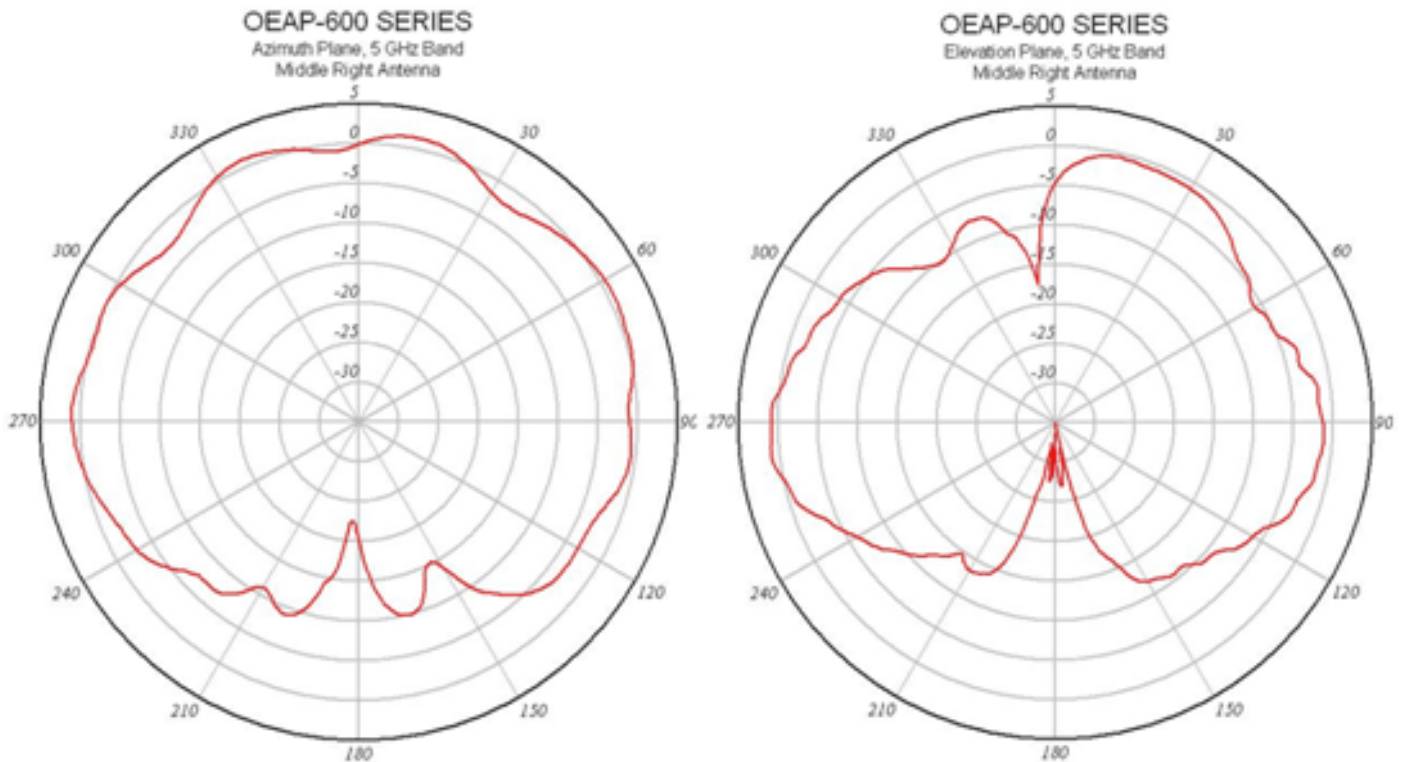
Het toegangspunt heeft zes antennes (drie per band).



Dit beeld toont een 2.4 GHz Antenne Stralingspatroon (genomen van de onderste linkerantenne).



Dit beeld toont een 5 GHz Antenne Stralingspatroon (genomen van de midden juiste antenne):



[Probleemoplossing voor APEE-600](#)

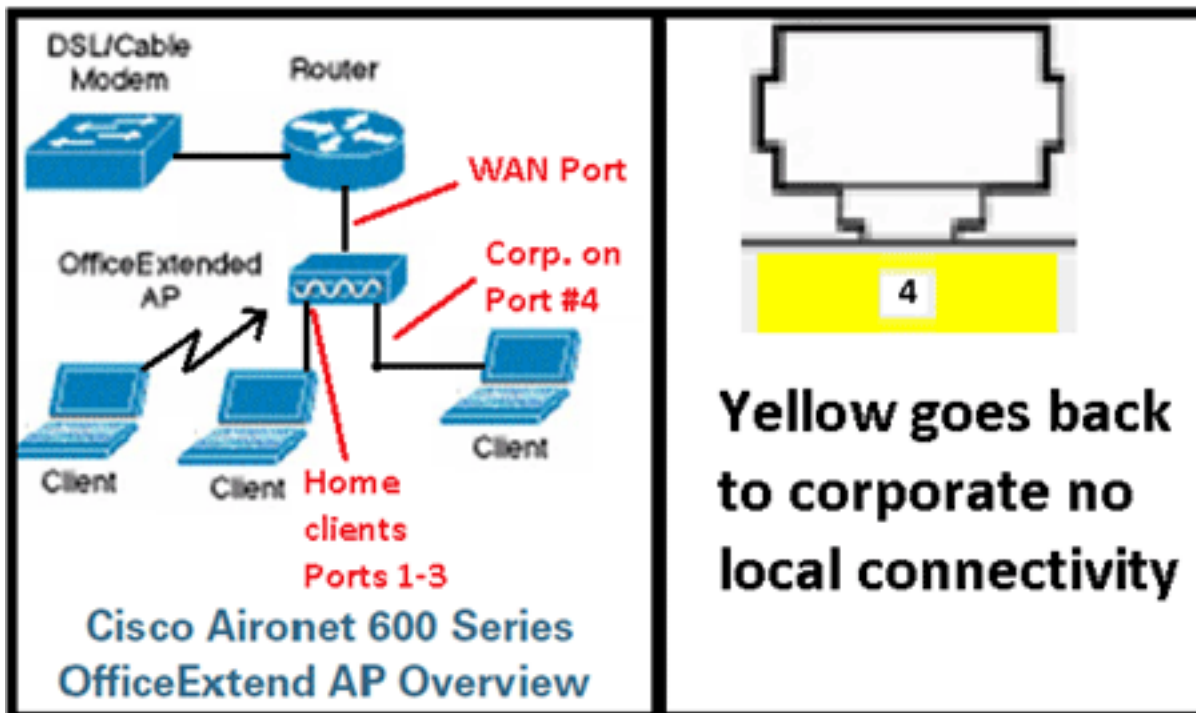
Controleer of de oorspronkelijke bedrading juist is. Dit bevestigt dat de WAN-poort op Cisco Aironet 600 Series APEE is aangesloten op de router en met succes een IP-adres kan ontvangen. Als het toegangspunt zich niet bij de controller lijkt aan te sluiten, sluit u een pc aan op poort 1-3 (thuisclientpoorten) en ziet u of u naar het toegangspunt kunt bladeren met het standaard IP-adres van 10.0.0.1. De standaardgebruikersnaam en het wachtwoord zijn admin.

Controleer of het IP-adres voor de bedrijfscontroller is ingesteld. Als dit niet het geval is, voert u het IP-adres in en start u de APEE van Cisco Aironet 600 Series opnieuw, zodat u kunt proberen een koppeling naar de controller te maken.

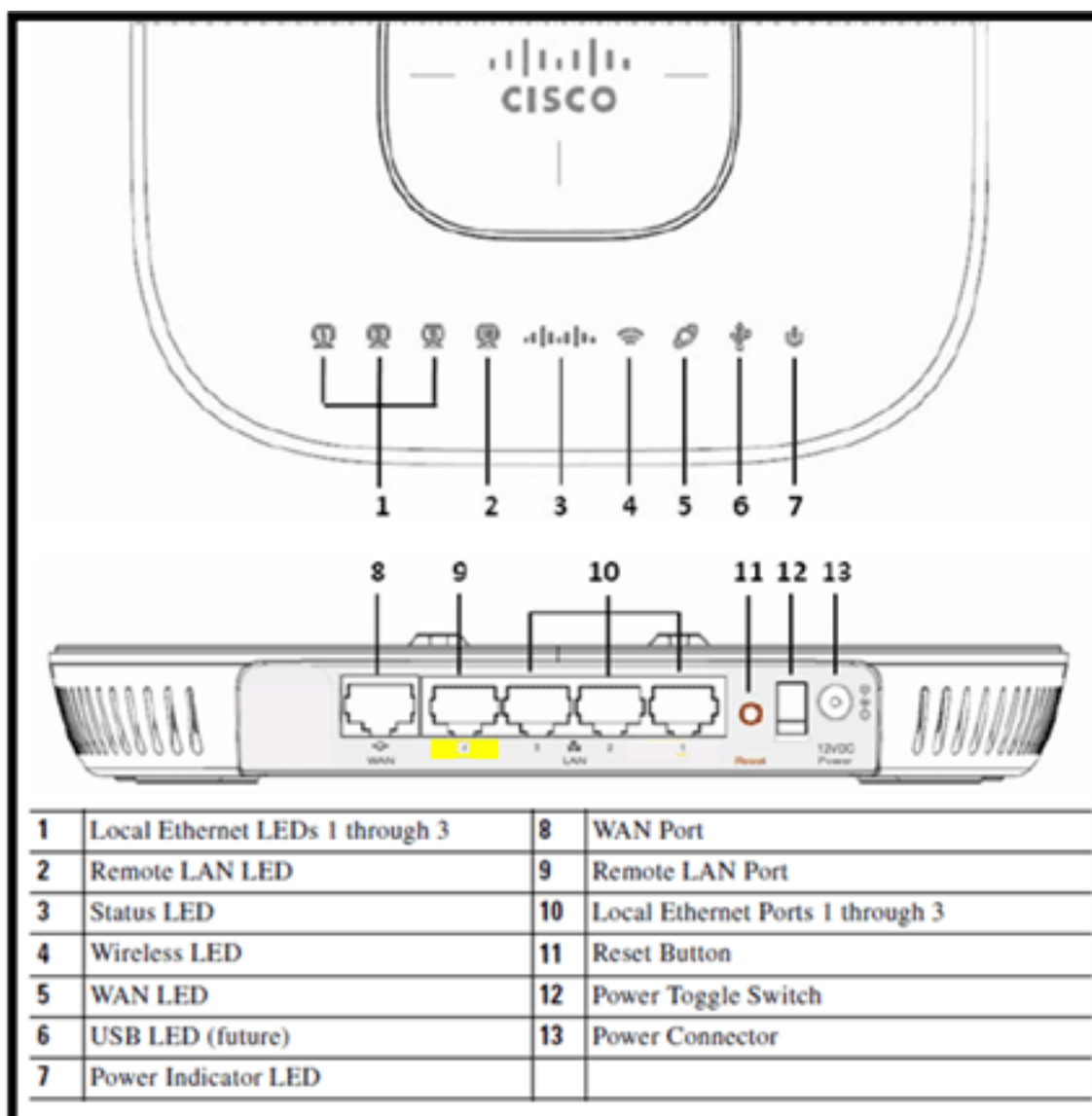
Opmerking: de #4 (in geel) kan niet worden gebruikt om naar het apparaat te bladeren voor configuratiedoeleinden. Dit is in essentie een "dode poort" tenzij een extern LAN is geconfigureerd. Vervolgens wordt de tunneling teruggedraaid naar het bedrijfsnetwerk (dat wordt gebruikt voor bekabelde ondernemingsconnectiviteit)

Controleer het gebeurtenissenlogboek om te zien hoe de associatie vorderde (meer hierover later).

Deze afbeelding toont het bedradingsdiagram van Cisco Aironet 600 Series OEAP:



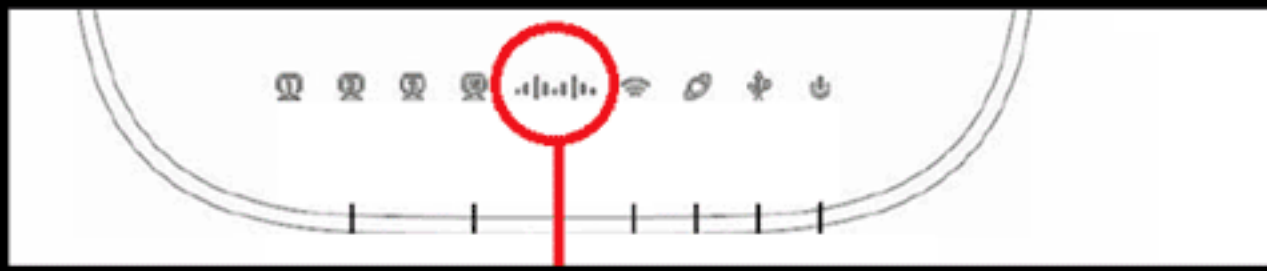
Deze afbeelding toont de Cisco Aironet 600 Series POE-connectiviteitspoorten:



Als Cisco Aironet 600 Series APEE er niet in slaagt zich aan te sluiten bij de controller, wordt aanbevolen om deze items te controleren:

1. Controleer of de router functioneel is en is aangesloten op de WAN-poort van Cisco Aironet 600 Series OEAP.
2. Sluit een PC aan op een van de poorten 1-3 op Cisco Aironet 600 Series OEAP. Het zou het internet moeten zien.
3. Controleer of het IP-adres van de controller van het bedrijf in het toegangspunt staat.
4. Bevestig dat de controller op DMZ staat en via het internet bereikbaar is.
5. Controleer of u meedoet en controleer of het Cisco-logo blauw of paars is.
6. Laat voldoende tijd voor het geval dat het toegangspunt een nieuw image moet laden en opnieuw moet starten.
7. Als een firewall in gebruik is, controleert u of de UDP 5246- en 5247-poorten niet zijn geblokkeerd.

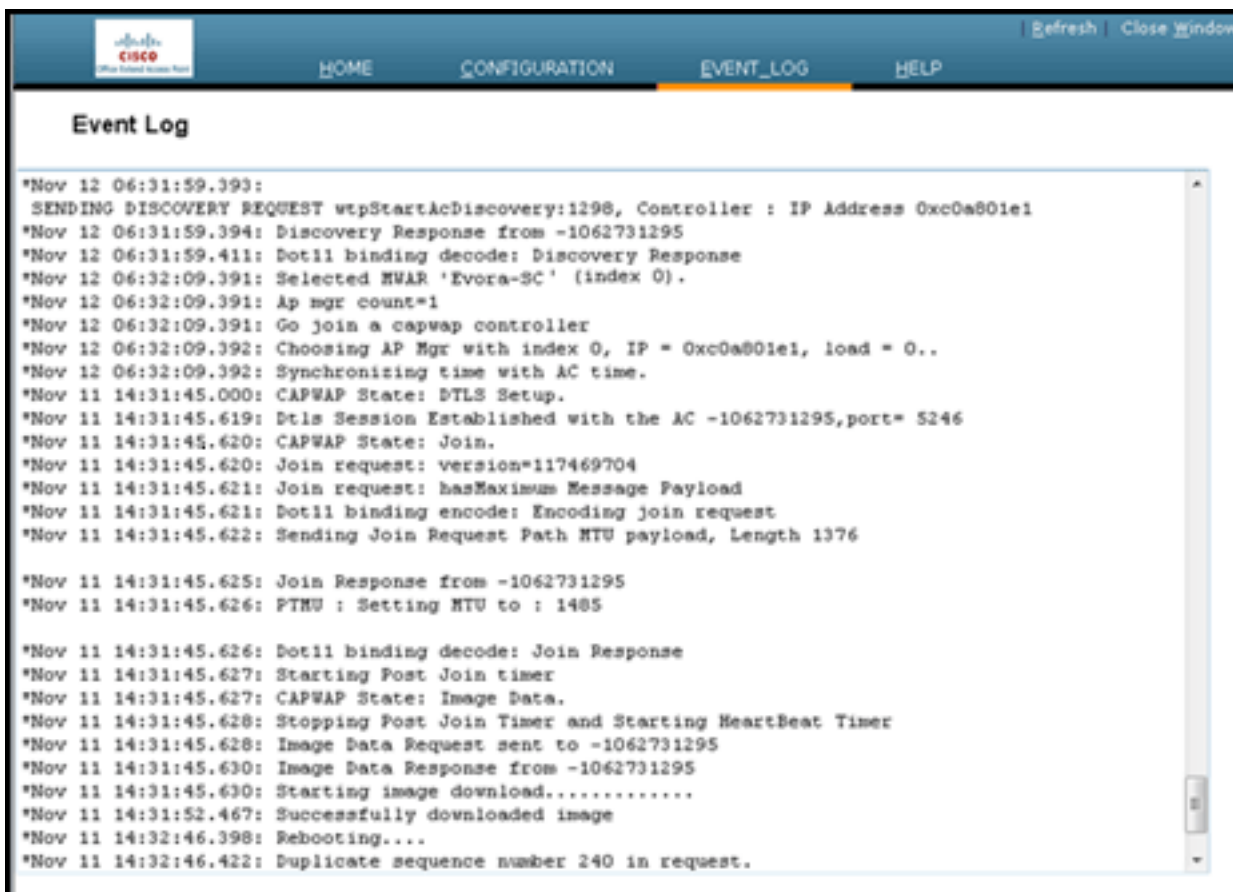
Deze afbeelding toont de LED-status van het OEAP-logo voor Cisco Aironet 600 Series:



Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing blue	Operating Status: Software upgrade in progress.
Flashing orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

Als het samenvoegen mislukt, knippert de LED door de kleuren of knippert wellicht oranje. Als dit zich voordoet, raadpleegt u het gebeurtenissenlogboek voor meer informatie. Blader naar het toegangspunt om het gebeurtenissenlogboek te bekijken (met behulp van persoonlijke SSID of bekabelde poorten 1-3) en leg deze gegevens vast zodat de IT-beheerder ze kan bekijken.

Deze afbeelding toont het gebeurtenissenlogboek van Cisco Aironet 600 Series OEAP:



Als het proces voor samenvoegen mislukt en dit de eerste keer is dat Cisco Aironet 600 Series APEE heeft geprobeerd verbinding te maken met de controller, controleer dan de statistieken voor samenvoeging van AP voor Cisco Aironet 600 Series APEE. Hiervoor hebt u de basisradio-MAC van het toegangspunt nodig. Dit kan worden gevonden in het gebeurtenissenlogboek. Hier is een voorbeeld van een gebeurtenissenlogboek met commentaar om u te helpen dit te interpreteren:

Event log 1

WAN port has not obtained IP address, otherwise it will be shown here.

AP Mac address

Base Radio MAC is 00:22:BD:DA:B6:00

```

*Jan 01 08:00:05.420: eth0  Linkencap:Ethernet HWaddrC0:C1:C0:05:48:86
*Jan 01 08:00:05.420:   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.420:   RX packets:1 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.420:   TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.421:   collisions:0 txqueuelen:100
*Jan 01 08:00:05.421:   RX bytes:64 (64.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.421:   Interrupt:4 Base address:0x2000
*Jan 01 08:00:05.444: eth1  Linkencap:Ethernet HWaddr00:22:BD:DA:B6:07
*Jan 01 08:00:05.444:   UP BROADCAST RUNNING ALLMULTI MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.444:   RX packets:0 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.444:   TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.444:   collisions:0 txqueuelen:100
*Jan 01 08:00:05.444:   RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.445:   Interrupt:3 Base address:0x1000
*Jan 01 08:00:05.467: Kernel IP routing table
*Jan 01 08:00:05.467: Destination Gateway Genmask Flags Metric Ref Use Iface
*Jan 01 08:00:05.467: 127.0.0.0 * 255.0.0.0 U 0 0 0 lo
*Jan 01 08:00:05.489: IP address HW type Flags HW address Mask Device
*Jan 01 08:00:05.540: oeap_mvar_ipaddr= Y.Y.Y.Y
*Jan 01 08:00:07.074: Subject: C=US, ST=California, L=San Jose, O=CISCO, OU=WNBU, CN=OEAP602-COC1C0054886/emailAd

```

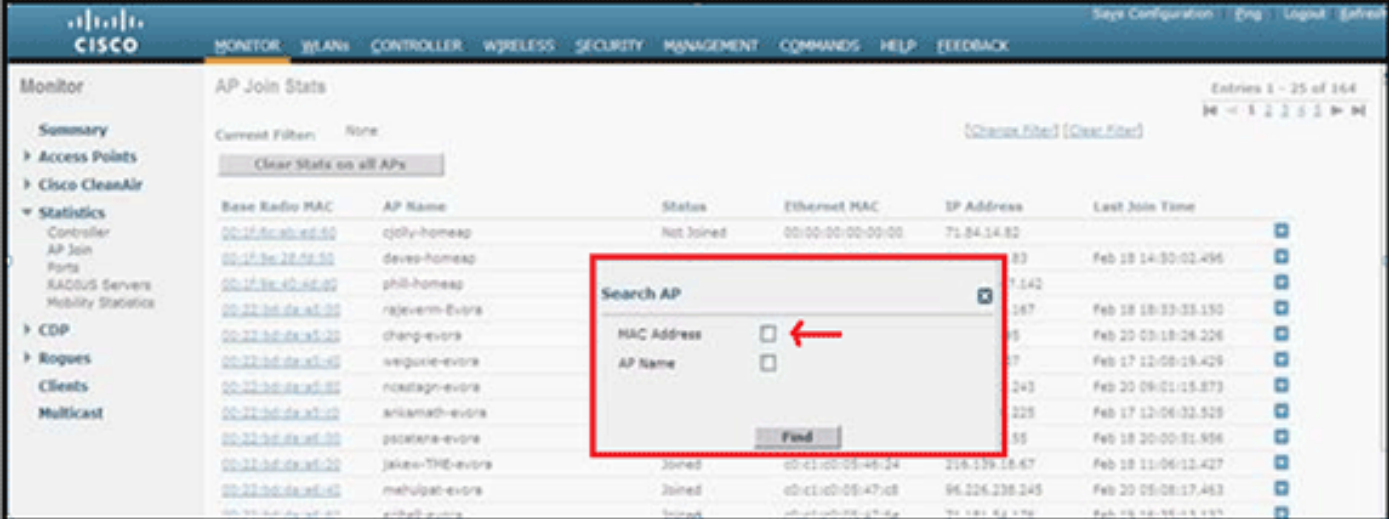
Controller IP address configured in local GUI

certificate

Zodra dit bekend is, kunt u in de statistieken van de controllermonitor kijken om te bepalen of Cisco Aironet 600 Series OEAP zich bij de controller heeft aangesloten of zich ooit bij de controller heeft aangesloten. Dit moet ook een indicatie geven waarom, of indien, een storing is opgetreden.

Als AP-verificatie vereist is, controleert u of het MAC-adres van Cisco Aironet 600 Series EAP Ethernet (niet het MAC-adres voor de radio) in kleine letters is ingevoerd in de Radius-server. U kunt het Ethernet MAC-adres ook vanuit het gebeurtenissenlogboek bepalen.

Zoeken op de controller voor Cisco Aironet 600 Series APEE



The screenshot shows the Cisco Controller Monitor interface. The main content area displays 'AP Join Stats' with a table of APs. A search dialog box is open, allowing users to search for APs by MAC Address or AP Name. A red arrow points to the 'MAC Address' input field in the search dialog.

Base Radio MAC	AP Name	Status	Ethernet MAC	IP Address	Last Join Time
00:1d:8c:9d:ed:00	qjoly-homeap	Not joined	00:00:00:00:00:00	71.84.14.82	
00:1d:8c:9d:ed:00	deves-homeap			83	Feb 18 14:30:02.495
00:1d:8c:9d:ed:00	phil-homeap			7,542	
00:1d:8c:9d:ed:00	rajevern-evora			187	Feb 18 18:33:33.150
00:1d:8c:9d:ed:00	chang-evora			45	Feb 20 03:18:26.226
00:1d:8c:9d:ed:00	vegore-evora			57	Feb 17 12:08:19.425
00:1d:8c:9d:ed:00	nostagn-evora			243	Feb 20 09:01:15.873
00:1d:8c:9d:ed:00	arlamath-evora			225	Feb 17 12:06:32.525
00:1d:8c:9d:ed:00	protona-evora			35	Feb 18 20:00:31.936
00:1d:8c:9d:ed:00	jakev-THE-evora	Joined	00:c1:00:09:46:24	218.179.18.67	Feb 18 11:06:12.427
00:1d:8c:9d:ed:00	mehulpat-evora	Joined	00:c1:00:09:47:c8	96.226.238.245	Feb 20 05:08:17.463
00:1d:8c:9d:ed:00	edibf-evora	Joined	00:1d:8c:9d:ed:00	71.84.14.82	Feb 18 05:45:03.197

Als u hebt vastgesteld dat internet toegankelijk is vanaf een pc die is aangesloten op de lokale Ethernet-poort, maar het toegangspunt nog steeds niet kan worden aangesloten bij de controller, en u hebt bevestigd dat het IP-adres van de controller is geconfigureerd in de lokale AP GUI en bereikbaar is, dan bevestig als het toegangspunt ooit met succes is aangesloten. Mogelijk bevindt het toegangspunt zich niet in de AAA-server. Of, als DTLS handshaking ontbreekt, kan AP een slechte certificaat of datum/tijdfout op het controlemechanisme hebben.

Als er geen Cisco Aironet 600 Series APEE-eenheden zich bij de controller kunnen aansluiten, controleert u of de controller op de DMZ bereikbaar is en of de UDP-poorten 5246 en 5247 geopend zijn.

[Hoe te debug client associatie problemen](#)

AP treedt op de juiste manier toe tot de controller, maar de draadloze client kan niet associëren met de Corporate SSID. Controleer het gebeurtenissenlogboek om te zien of een associatiebericht het toegangspunt bereikt.

Het volgende cijfer toont de normale gebeurtenissen voor cliëntvereniging met collectieve SSID met WPA of WPA2. Voor SSID met open authenticatie of statische WEP, is er slechts één ADD MOBIËLE gebeurtenis.

gebeurtenissenlogboek - Clientassociatie

```
*Feb 19 20:26:58.876: (Re)Assoc-Req from 00:24:d7:2a:72:c0 forwarded to WLC, wired: no
*Feb 19 20:26:58.941: received assoc-rsp for wireless client, status=0000
*Feb 19 20:26:58.942:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1
*Feb 19 20:26:58.942: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
*Feb 19 20:27:00.648:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=4
*Feb 19 20:27:00.649: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
```

Als er geen (Re)Assoc-Req-gebeurtenis in het logbestand staat, controleert u of de client de juiste beveiligingsinstellingen heeft.

Als de gebeurtenis (Re)Assoc-Req in het logbestand verschijnt maar de client niet goed kan koppelen, schakelt u de opdracht **debug client <MAC-adres>** op de controller voor de client in en onderzoekt u het probleem op dezelfde manier als een client die werkt met andere Cisco-toegangspunten die niet OEAP zijn.

[Hoe het gebeurtenissenlogboek te interpreteren](#)

De volgende logboeken met opmerkingen kunnen u helpen bij het oplossen van problemen met andere Cisco Aironet 600 Series OEAP-verbindingsproblemen.

Hier zijn een paar voorbeelden van voorbeelden die zijn verzameld uit de logbestanden van de gebeurtenissen in Cisco Aironet 600 Series OEAP met commentaar om te helpen bij de interpretatie van het gebeurtenissenlogboek:

Event log 2

*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
*Jan 01 08:00:08.975: CAPWAP State: Init.
*Jan 01 08:00:09.009: CAPWAP State: Discovery.
*Jan 01 08:00:09.042: Starting Discovery.
*Jan 01 08:00:09.044: CAPWAP State: Discovery.
*Jan 01 08:00:09.193: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194: SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address:
*Jan 01 08:00:09.195: Discovery Request sent to Y.Y.Y.Y with discovery type set to 0
*Jan 01 08:00:09.256: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.272: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.273: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
*Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Ap mgr count=1
*Jan 01 08:00:19.183: Go join a capwap controller
*Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = Y.Y.Y.Y , load=151.
*Jan 01 08:00:19.183: Synchronizing time with AC time.
*Feb 19 23:33:56.000: CAPWAP State: DTLS Setup.
*Feb 19 23:34:16.813: Dtls Session Established with the AC: Y.Y.Y.Y , port= 5246

Discovery Request sent
If AP can not get IP address,
then Discovery Req. will not be sent

Discovery resp. received from
controller. If no response from
controller, then need to check
whether controller
is accessible

Selected controller to join, timestamp synced to the controller

DTLS handshaking with the controller
completed. If certificate has problem, then
the failure will happen here

Event log 3

*Feb 19 23:34:16.813: CAPWAP State: Join.
*Feb 19 23:34:16.814: Join request: version=7.0.114.76

*Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
*Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
*Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376

*Feb 19 23:34:16.887: Join Response from Y.Y.Y.Y
*Feb 19 23:34:16.888: PTMU : Setting MTU to : 1485

*Feb 19 23:34:16.888: Dot11 binding decode: Join Response
*Feb 19 23:34:16.889: Starting Post Join timer
*Feb 19 23:34:16.890: CAPWAP State: Image Data.
*Feb 19 23:34:16.890: Controller Version: 7.0.114.76
*Feb 19 23:34:16.890: AP Version: 7.0.114.76
*Feb 19 23:34:16.891: CAPWAP State: Configure.
*Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
*Feb 19 23:34:16.893: hwapp_encode_ap_reset_button_payload: reset button state off
*Feb 19 23:34:16.895: Configuration Status sent to Y.Y.Y.Y
*Feb 19 23:34:17.019: Configuration Status Response from Y.Y.Y.Y
*Feb 19 23:34:17.022: CAPWAP State: Run.
*Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
*Feb 19 23:34:17.023: CAPWAP State: Run.

Join Resp. from controller
If AP is not added to AAA server,
this step will fail.

Controller and AP have same version
SW, no image download is need. When
controller is upgraded to new version
SW, image download will happen.

Capwap configuration completes

Event log 4

```
*Feb 19 23:34:17.023: CAPWAP moved to RUN state stopping post join timer
*Feb 19 23:34:17.399: capwapWtpDlForwarding() returned 1
*Feb 19 23:34:17.602: capwapWtpDlForwarding() returned 1
*Feb 19 23:34:17.762: Change State Event Response from -1421466749
*Feb 19 23:34:17.853: SSID alpha,WLAN ID 1, added to the slot[0], enabled
*Feb 19 23:34:18.045: SSID alpha_phone,WLAN ID 2, added to the slot[0], enabled
*Feb 19 23:34:18.118: Ethernet Backhaul WLAN ID = 3,qos=0
*Feb 19 23:34:18.281: SSID alpha,WLAN ID 1, added to the slot[1], enabled
*Feb 19 23:34:18.522: SSID alpha_phone,WLAN ID 2, added to the slot[1], enabled
```

WLANs are configured for 2.4 GHz Radio

Remote-lan is configured

WLANs are configured for 5 GHz Radio

Wanneer de internetverbinding onbetrouwbaar lijkt

Het voorbeeld van het gebeurtenislogboek in deze sectie kan voorkomen wanneer de internetverbinding mislukt of zeer traag of intermitterend wordt. Dit kan worden veroorzaakt door uw ISP-netwerk, de ISP-modem of uw thuisrouter. Soms daalt de verbinding van de ISP of wordt onbetrouwbaar. Wanneer dit gebeurt, kan de CAPWAP-link (tunnel terug naar het bedrijf) falen of problemen hebben.

Hier is een voorbeeld van een dergelijke fout in het gebeurtenissenlogboek:

```
*Feb 16 07:13:24.918: Re-Tx Count= 0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count= 4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808)., 2}
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count= 6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808)
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAPState: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

Aanvullende debug-opdrachten

Wanneer u de Cisco Aironet 600 Series APEE in een hotel of andere betaallocatie gebruikt, moet u door de ommuurde tuin gaan voordat de Cisco Aironet 600 Series APEE terug naar de controller kan tunnelen. Sluit hiervoor een laptop aan op een van de bekabelde lokale poorten (poort 1-3) of gebruik een persoonlijke SSID om in te loggen op het hotel en het spatscherm tevreden te stellen.

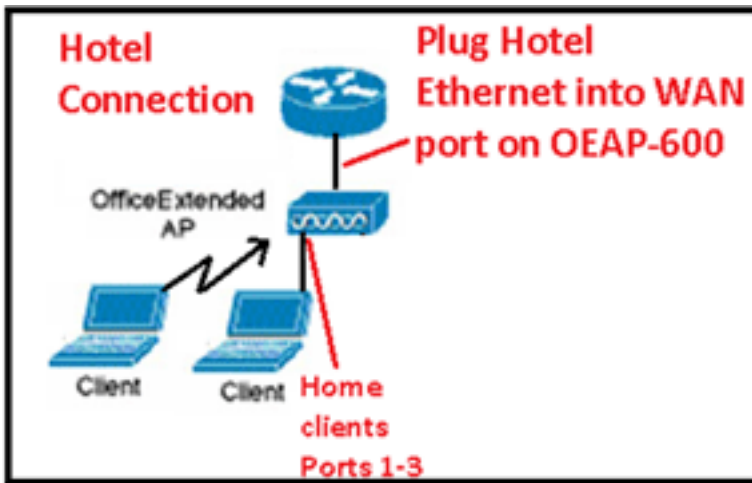
Zodra u internetverbinding hebt vanaf de thuishant van de AP, creëert de unit een DTLS-tunnel en uw zakelijke SSID's. Vervolgens wordt de bekabelde #4 (ervan uitgaande dat een extern LAN is geconfigureerd) actief.

Opmerking: dit kan een paar minuten duren, kijk naar het Cisco-logo LED voor solide blauw of paars om aan te geven dat u succesvol meedoet. Op dit moment zijn zowel persoonlijke als

zakelijke connectiviteit actief.

Opmerking: de tunnel breekt als hotel of een andere ISP de verbinding verbreekt (meestal 24 uur). Dan moet je hetzelfde proces opnieuw starten. Dit is door ontwerp en is normaal.

Dit beeld toont Office Extend in pay-for-use configuratie:



Deze afbeelding toont aanvullende debug-opdrachten (informatie over de radio-interface):

```
Below are the new diagnostics commands for the OEAP 600

The WLC CLI of "show tech" is:
debugap enable <apname>
then:
debugap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
debugap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
debugap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)

The "show eventlog" is the same as other APs:
show ap eventlog <apname>
```

[Bekende problemen/voorbehoud](#)

Wanneer u het configuratiebestand van een controller naar een TFTP/FTP-server uploadt, worden Remote-LAN-configuraties geüpload als WLAN-configuraties. Raadpleeg [Releaseopmerkingen voor Cisco draadloze LAN-controllers en lichtgewicht access points voor release 7.0.16.0](#) voor meer informatie.

Als de CAPWAP-verbinding op de OEAP-600 uitvalt als gevolg van een verificatiefout op de controller, kan het Cisco-logo-LED op de OEAP-600 enige tijd worden uitgeschakeld voordat de OEAP-600 de CAPWAP-poging opnieuw probeert te starten. Dit is normaal, dus je moet weten dat de AP niet is gestorven als het logo LED tijdelijk wordt uitgeschakeld.

Dit OEAP-600-product heeft een andere inlognaam dan de vorige OEAP Access points, zodat het consistent is met thuisproducten zoals Linksys. De standaardgebruikersnaam is *admin* met een wachtwoord van *admin*. De andere Cisco OEAP Access points zoals de AP-1130 en AP-1140 hebben een standaardgebruikersnaam van *Cisco* met een wachtwoord van *Cisco*.

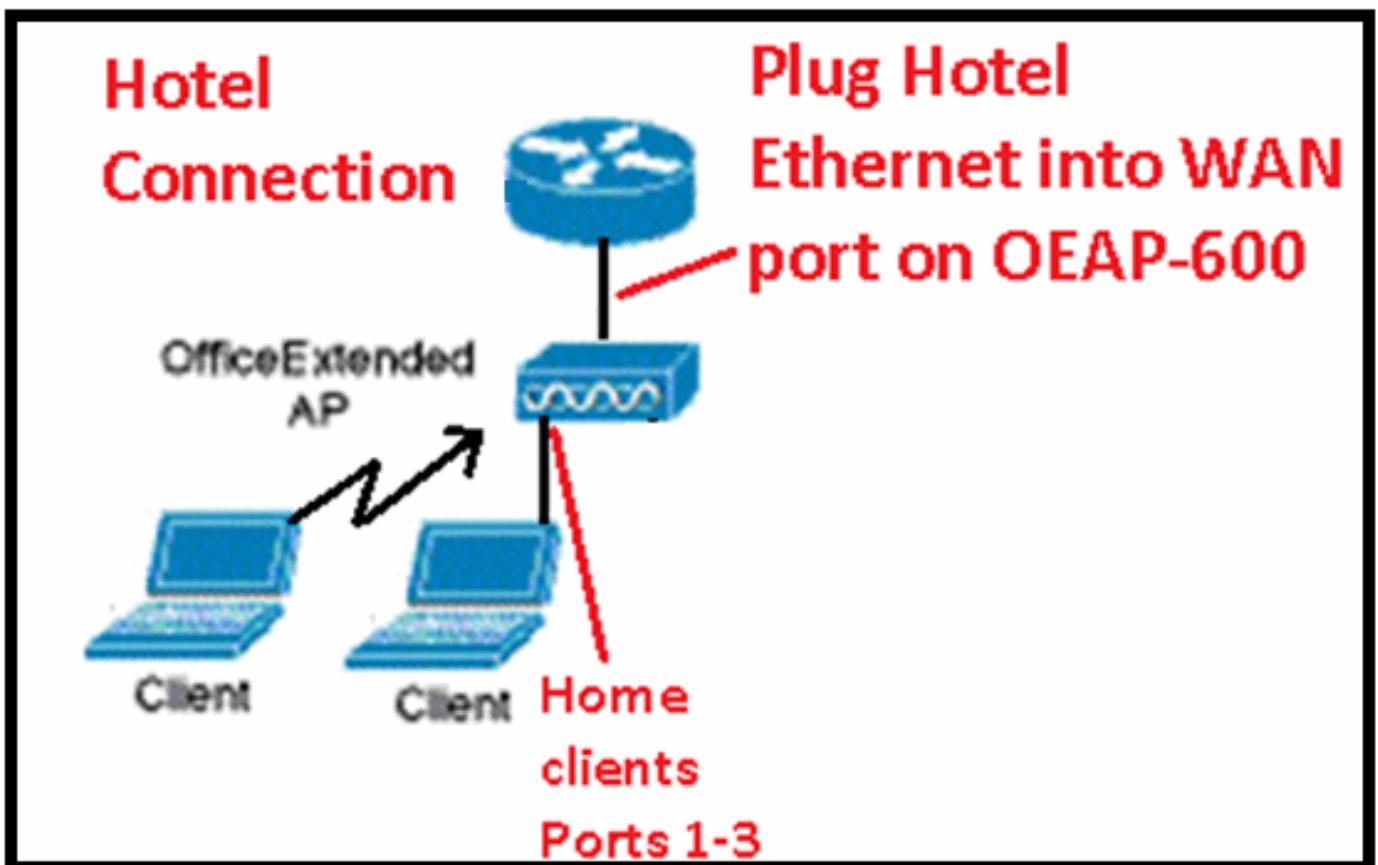
Deze eerste release van de OEAP-600 heeft 802.1x-ondersteuning, maar wordt alleen

ondersteund op de CLI. Gebruikers die proberen wijzigingen aan te brengen in de GUI, kunnen hun configuraties verliezen.

Wanneer u de OEAP-600 gebruikt in een hotel of andere betaallocatie, voordat de OEAP-600 terug kan tunnelen naar de controller, moet u door de ommuurde tuin. Sluit gewoon een laptop aan op een van de bekabelde lokale poorten (poort 1-3) of gebruik een persoonlijk SSID log in het hotel en maak het spatscherm tevreden. Zodra u internetverbinding hebt vanaf de thuishant van het toegangspunt, creëert de unit vervolgens een DTLS-tunnel en uw bedrijfs-SSID's en bekabelde #4, die ervan uitgaat dat Remote-LAN is geconfigureerd, dan wordt het actief. Houd er rekening mee dat dit een paar minuten kan duren. Let op dat u de LED van het Cisco-logo voor effen blauw of paars gebruikt om aan te geven dat de deelname succesvol is. Op dit moment zijn zowel persoonlijke als zakelijke connectiviteit actief.

Opmerking: de tunnel kan breken wanneer hotel of andere ISP losmaakt (meestal 24 uur) en je zou hetzelfde proces opnieuw moeten starten. Dit is door ontwerp en is normaal.

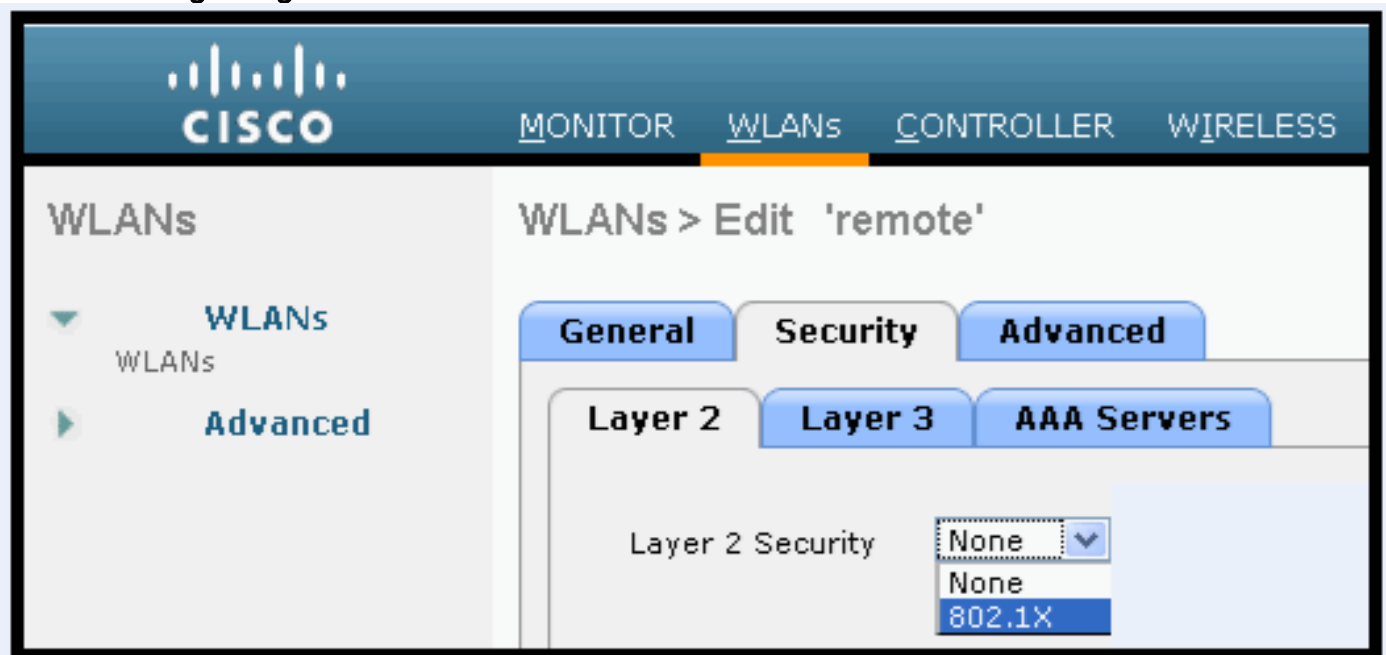
Office Extend in pay voor gebruik locatie



Dit zijn enkele extra verbeteringen die in de Cisco 7.2-release zijn geïntroduceerd:

- Toevoeging van 802.1x-beveiliging toegevoegd in GUI
- Mogelijkheid om lokale WLAN-toegang op de AP uit te schakelen van controller - persoonlijke SSID uitschakelen, alleen bedrijfconfiguratie toestaan
- Selecteerbare opties voor kanaaltoewijzing
- Ondersteuning gewijzigd van 2 collectieve SSID naar 3 SSID's
- Ondersteuning voor twee LAN-poortfuncties

Toevoeging van 802.1x-beveiliging toegevoegd in GUI



Opmerkingen met betrekking tot verificatie voor externe LAN-poort.

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

Mogelijkheid om lokale WLAN-toegang op de AP uit te schakelen van controller - persoonlijke SSID uitschakelen, alleen bedrijfconfiguratie toestaan

Lokale WLAN-toegang uitschakelen

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The 'Global Configuration' page is displayed, with the 'GEAP Config Parameters' section highlighted by a red circle. In this section, the 'Disable local APs' checkbox is checked, indicating that the APs are managed locally. Other sections visible include CDP, High Availability, and Login Credentials.

De geselecteerde opties voor kanaaltoewijzing zijn:

- AP, lokaal bestuurd
- WLC-gestuurd

RF-kanaal- en voedingstoewijzingen nu lokaal of WLC-gestuurd

The screenshot shows the configuration page for a specific AP (802.11a/n Cisco APs > Configure). The 'RF Channel Assignment' and 'Tx Power Level Assignment' sections are highlighted by a red circle. In the 'RF Channel Assignment' section, the 'Assignment Method' is set to 'WLC Controlled'. In the 'Tx Power Level Assignment' section, the 'Assignment Method' is also set to 'WLC Controlled'. Other sections visible include General, 11n Parameters, and CleanAir.

Manually configure channel and power level

In JMR1 release, there is no configuration option for 802.11a/n and 802.11b/g/n radios for the OEAP-600 AP. In 7.2 release; the configuration window is added back with only "General", "RF Channel Assignment" and "Tx Power Level Assignment" portions. The "Admin Status" in "General" shall be display only. The options for "Assign Method" are changed to "Custom Configured" and "AP Controlled". By default "AP Controlled" is selected. Channel and Tx power level can be configured only when they are in "Custom Configured" mode.

OEAP-600 does not support DFS channels so that WLC shall not allow these channels to be configured. [This new assignment method is passed to AP with CAPWAP payload.

In AP, when the channel is "AP Controlled", then the channel is controlled by the setting from local AP GUI. Otherwise the channel set by WCS is used.

The channel assign method and the assigned channel are saved in NVRAM and displayed in local GUI.

In AP, when the power is "AP controlled", then the maximum power level is always used. Otherwise the power level set by WCS is used.

The assign method for TX power level and assigned TX power level shall be saved in flash so that they can take effect after AP reboots.

When "Reset to Default" operation is performed, the assign method is set to "AP controlled".

Ondersteuning voor twee LAN-poortfuncties (alleen CLI)

Deze opmerking is van toepassing op AP's uit de EAP-600-reeks die gebruikmaken van de functie Dual LAN-poorten, waarmee EAP-600 Ethernet-poort 3 kan fungeren als een extern LAN. De configuratie is alleen toegestaan via de CLI, en hier is een voorbeeld:

```
Config network oeap-600 dual-rlan-ports enable|disable
```

In het geval dat deze functie niet is geconfigureerd, blijft het enige poort 4-afstandsbediening functioneren. Elke poort gebruikt een uniek remote-plan voor elke poort. De remote-lan afbeelding is anders, wat er afhankelijk van is of de standaard-groep of AP Groepen wordt gebruikt.

Standaard groep

Als de standaardgroep wordt gebruikt, wordt één externe LAN met een even externe LAN-id toegewezen aan poort 4. Het remote-lan met remote-lan-id 2 wordt bijvoorbeeld toegewezen aan poort 4 (op de OEAP-600). Het remote-lan met een oneven nummerde remote-lan-ID wordt toegewezen aan poort 3 (op de OEAP-600).

Neem als voorbeeld deze twee afstandsbedieningen:

(Cisco Controller) >show remote-lan summary

Number of Remote LANS..... 2

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

rlan2 heeft een even genummerde remote-lan ID, 2, en als zulke kaarten naar poort 4. rlan3 heeft oneven remote-lan ID 3, en dus kaarten naar poort 3.

AP-groepen

Als u een AP-groep gebruikt, wordt de toewijzing aan de EAP-600-poorten bepaald door de opdracht AP-groep. Als u een AP-groep wilt gebruiken, moet u eerst alle afstandsbedieningen en WLAN's uit de AP-groep verwijderen en leeg laten. Voeg vervolgens de twee afstandsbedieningen toe aan de AP-groep. Voeg eerst de poort 3 AP Remote-LAN toe, voeg vervolgens poort 4 Remote Group toe en voeg uiteindelijk alle WLAN's toe.

Een remote-lan in de eerste positie in de lijst kaarten naar poort 3, en de tweede in de lijst kaarten naar poort 4, zoals in dit voorbeeld:

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

Gerelateerde informatie

- [Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.