

Configuratievoorbeeld van draadloze LAN-controllers mesh

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Cisco Aironet 1510 Series lichtgewicht mesh access point voor buitengebruik](#)

[Aironet 1000 access point \(RAP\)](#)

[PoE-top access point \(PAP\)](#)

[Functies die niet op mesh-netwerken worden ondersteund](#)

[Opstartvolgorde voor access point](#)

[Configureren](#)

[Configuratie nulpunt inschakelen \(standaard ingeschakeld\)](#)

[Voeg de MIC toe aan de AP Authorized List](#)

[Overbruggingsparameters voor APs configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document biedt een basisconfiguratievoorbeeld voor het maken van een point-to-point gebrugde link met behulp van de mesh-netwerkoplossing. Dit voorbeeld gebruikt twee lichtgewicht access point (LAP's). Eén LAP opereert als een dak-top access point (RAP), de andere LAP opereert als een peer-top access point (PAP) en ze worden aangesloten op een Cisco Wireless LAN (WLAN) controller (WLC). De RAP is verbonden met de WLC door een Cisco Catalyst switch.

Raadpleeg het gedeelte [Netwerkconfiguratie voor draadloze LAN-controllers voor mesh voor release 5.2 en hoger](#) voor WLC release 5.2 en latere versies

[Voorwaarden](#)

- De WLC is ingesteld voor een eenvoudige bediening.
- De WLC wordt ingesteld in Layer 3-modus.
- De switch voor de WLC is ingesteld.

Vereisten

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

- Basiskennis van de configuratie van LAN's en Cisco WLC's
- Basiskennis van Lichtgewicht AP Protocol (LWAPP).
- Kennis van de configuratie van een externe DHCP-server en/of domeinnaamserver (DNS)
- Basisconfiguratiekennis van Cisco-switches

Gebruikte componenten

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

- Cisco 4402 Series WLC-software met firmware 3.2.150.6
- Twee (2) Cisco Aironet 1510 Series LAP's
- Cisco Layer 2 Switch

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

Cisco Aironet 1510 Series lichtgewicht mesh access point voor buitengebruik

De Cisco Aironet 1510 Series lichtgewicht mesh-AP voor buitengebruik is een draadloos apparaat dat is ontworpen voor draadloze clienttoegang en point-to-point bridging, point-to-multipoint bridging en point-to-multipoint mesh draadloze connectiviteit. Het toegangspunt voor buitengebruik is een standalone unit die op een muur of overhang, op een dak of op een lichtstok op straat kan worden gemonteerd.

AP1510 werkt met controllers om gecentraliseerd en schaalbaar beheer, hoge veiligheid, en mobiliteit te verstrekken. Ontworpen om implementaties met een nulconfiguratie te ondersteunen, sluit AP1510 zich gemakkelijk en veilig aan bij het netwerk van het netwerk en is beschikbaar om het netwerk te beheren en te bewaken via de controller GUI of CLI.

De AP1510 is uitgerust met twee tegelijkertijd bediende radio's: een 2,4-GHz radio gebruikt voor clienttoegang en een 5-GHz radio gebruikt voor gegevensbackhaul naar andere AP1510s. Draadloos LAN-clientverkeer passeert via de backhaul-radio van het AP of wordt via andere AP1510s doorgegeven tot het de Ethernet-verbinding van de controller bereikt.

Aironet 1000 access point (RAP)

RAP's hebben een bekabelde verbinding met een Cisco WLC. Ze gebruiken de backhaul

draadloze interface om te communiceren met naburige PAP's. RAP's zijn het ouderknooppunt voor een overbruggingsnetwerk of een netwerk met mazen en sluiten een brug- of netwerk aan op het bekabelde netwerk. Daarom kan er slechts één RAP zijn voor elk overbrugd of vermaasd netwerksegment.

N.B.: Wanneer u de netwerkoplossing voor LAN-to-LAN overbrugging gebruikt, sluit u geen RAP rechtstreeks aan op een Cisco WLC. Een switch of router tussen de Cisco WLC en de RAP is vereist omdat Cisco WLCs geen Ethernet verkeer verzenden dat van een aan LWAPP verbonden poort komt. RAP's kunnen werken in Layer 2 of Layer 3 LWAPP-modus.

PoE-top access point (PAP)

PAP's hebben geen bekabelde verbinding met een Cisco WLC. Ze kunnen volledig draadloos zijn en klanten ondersteunen die communiceren met andere PAP's of RAP's, of ze kunnen worden gebruikt om verbinding te maken met perifere apparaten of een bekabeld netwerk. De Ethernet poort is om veiligheidsredenen gehandicapt maar u zou het voor PAPs moeten toelaten.

Opmerking: Cisco Aironet 1030 Remote Edge LAP's ondersteunen single-hop-implementaties terwijl Cisco Aironet 1500 Series lichtgewicht access points voor buitengebruik zowel single-mode als multi-hop implementaties ondersteunen. Als dergelijk, kan Cisco Aironet 1500 Series Lichtgewicht access points voor buitengebruik als dak worden gebruikt als AP's en als PAP's voor een of meer hop uit Cisco WLC.

Functies die niet op mesh-netwerken worden ondersteund

Deze controllers worden niet ondersteund op vermaasde netwerken:

- Ondersteuning voor meerdere landen
- Op lading gebaseerde CAC (mesh-netwerken ondersteunen alleen op bandbreedte gebaseerd of statisch, CAC.)
- Hoge beschikbaarheid (snelle hartslag en primaire ontdekking voegen-timer)
- EAP-FASTv1- en 802.1X-verificatie
- EAP-FASTv1- en 802.1X-verificatie
- Lokaal significant certificaat
- Plaatselijke diensten

Opstartvolgorde voor access point

In deze lijst wordt beschreven wat er gebeurt bij het starten van de RAP- en PAP-programma's:

- Al het verkeer reist door de RAP en de WLC van Cisco voordat het naar het LAN wordt verzonden.
- Wanneer de RAP omhoog komt, verbinden de PAP's er automatisch mee.
- De aangesloten link gebruikt een gedeeld geheim om een sleutel te genereren die wordt gebruikt om Advanced Encryption Standard (AES) te leveren voor de link.
- Zodra de afstandsPAP op de RAP is aangesloten, kunnen APs van het netwerk gegevensverkeer doorgeven.
- De gebruikers kunnen het gedeelde geheim wijzigen of de access points van het netwerk configureren met behulp van de Cisco opdrachtregel interface (CLI), de Cisco web user

interface van de controller of het Cisco Wireless Control System (Cisco WCS). Cisco raadt u aan het gedeelde geheim te wijzigen.



Configureren

Voltooi deze stappen om de WLC en de APs voor point-to-point bridging te configureren.

1. [Configuratie nulpunt inschakelen op de WLC.](#)
2. [Voeg de MIC toe aan de AP autorisatie lijst.](#)
3. [Configureren van overbruggparameters voor de AP's.](#)
4. [Controleer de configuratie.](#)

Configuratie nulpunt inschakelen (standaard ingeschakeld)

GUI-configuratie

Met Zero Touch Configuration kunnen de AP's de gedeelde geheime sleutel van de controller verkrijgen wanneer deze wordt geregistreerd met de WLC. Als u het vakje uitschakelt, biedt de controller niet de gedeelde geheime sleutel en gebruiken de AP's een standaard vooraf gedeelde sleutel voor beveiligde communicatie. De standaardwaarde is ingeschakeld (of afgevinkt). Volg deze stappen vanuit de WLC GUI:

Opmerking: In WLC versie 4.1 en hoger is geen optie voor Zero-Touch-configuratie.

1. Kies **Draadloos > overbruggen** en klik op **Configuratie nulpunt inschakelen**.
2. Selecteer het sleutelformaat.
3. Geef de overbruggingssleutel op.
4. Voer de overbrugging gedeelde sleutel opnieuw in in de Bevestigde Gedeeld Sleutel.

Wireless

Access Points
 All APs
 802.11a Radios
 802.11b/g Radios
 Third Party APs

Bridging

Rogues
 Rogue APs
 Known Rogue APs
 Rogue Clients
 Adhoc Rogues

Clients

Global RF
 802.11a Network
 802.11b/g Network
 802.11h

Country

Timers

Bridging

Zero Touch Configuration

Enable Zero Touch Configuration

Key Format ASCII ▾

Bridging Shared Secret Key ●●●

Confirm Shared Secret Key ●●●

CLI-configuratie

Volg deze stappen van de CLI:

1. Geef de **configuratie van het netwerk toe-op** het **configuratie van het netwerk-nulinstelling**.
 (Cisco Controller) `>config network zero-config enable`
2. Geef het **configuratie netwerk overbrugging-gedeeld-geheim <string>** uit om de overbruggingsgedeelde geheime sleutel toe te voegen.
 (Cisco Controller) `>config network bridging-shared-secret Cisco`

[Voeg de MIC toe aan de AP Authorized List](#)

De volgende stap is het toevoegen van AP aan de machtigingslijst op de WLC. Om dit te doen, kies **Beveiliging > AP Beleid**, voer het AP MAC adres in onder Toevoegen AP aan de Lijst van de Vergunning en klik **Toevoegen**.

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

AP Policies

Policy Configuration

Authorize APs against AAA Enabled

Accept Self Signed Certificate Enabled

Apply

Add AP to Authorization List

MAC Address

Certificate Type

Add

AP Authorization List Items 0 to 20 of 0

MAC Address	Certificate Type	SHA1 Key Hash
-------------	------------------	---------------

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

AP Policies

Policy Configuration

Authorize APs against AAA Enabled

Accept Self Signed Certificate Enabled

Add AP to Authorization List

MAC Address

Certificate Type

AP Authorization List Items 1 to 2 of 2

MAC Address	Certificate Type	SHA1 Key Hash
00:0b:85:5e:40:00	MIC	
00:0b:85:5e:5a:80	MIC	

In dit voorbeeld worden zowel AP's (de RAP en de PAP) toegevoegd aan de AP-autorisatielijst op de controller.

CLI-configuratie

Geef de configuratie **auth-list toe de opdracht mic <AP mac>** toe om de MIC aan de autorisatielijst toe te voegen.

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80
```

Configuratie

Dit document gebruikt deze configuratie:

Cisco WLC 4402 router

```
(Cisco Controller) >show run-config
```

```
Press Enter to continue...
```

System Inventory

```
Switch Description..... Cisco  
Controller  
Machine Model.....  
WLC4402-12  
Serial Number.....  
FLS0943H005  
Burned-in MAC Address.....  
00:0B:85:40:CF:A0  
Crypto Accelerator 1..... Absent  
Crypto Accelerator 2..... Absent  
Power Supply 1..... Absent  
Power Supply 2.....  
Present, OK
```

```
Press Enter to continue Or <Ctl Z> to abort
```

System Information

```
Manufacturer's Name..... Cisco  
Systems, Inc  
Product Name..... Cisco  
Controller  
Product Version.....  
3.2.150.6  
RTOS Version.....  
3.2.150.6  
Bootloader Version.....  
3.2.150.6  
Build Type..... DATA +  
WPS  
  
System Name.....  
lab120wlc4402ip100  
System Location.....  
System Contact.....  
System ObjectID.....  
1.3.6.1.4.1.14179.1.1.4.3  
IP Address.....  
192.168.120.100  
System Up Time..... 0 days  
1 hrs 4 mins 6 secs  
  
Configured Country..... United  
States  
Operating Environment.....  
Commercial (0 to 40 C)  
Internal Temp Alarm Limits..... 0 to  
65 C  
Internal Temperature..... +42 C
```

State of 802.11b Network.....
Disabled
State of 802.11a Network.....
Disabled
Number of WLANs..... 1
3rd Party Access Point Support.....
Disabled
Number of Active Clients..... 0

Press Enter to continue Or <Ctl Z> to abort

Switch Configuration

802.3x Flow Control Mode.....
Disable
Current LWAPP Transport Mode..... Layer
3
LWAPP Transport Mode after next switch reboot.... Layer
3
FIPS prerequisite features.....
Disabled

Press Enter to continue Or <Ctl Z> to abort

Network Information

RF-Network Name..... airespacerf
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable
Mode: Ucast
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Enable
Bridge AP Zero Config..... Enable
Bridge Shared Secret.....
youshouldsetme
Allow Old Bridging Aps To Authenticate..... Disable
Over The Air Provisioning of AP's..... Disable
Mobile Peer to Peer Blocking..... Disable
Apple Talk Disable
AP Fallback Enable
Web Auth Redirect Ports 80
Fast SSID Change Disabled

Press Enter to continue Or <Ctl Z> to abort

Port Summary

	STP	Admin	Physical	Physical	Link
Link	Mcast				
Pr	Type	Stat	Mode	Status	Status
Trap	Appliance	POE			
1	Normal	Forw	Enable	Auto	1000 Full Up
	Enable	Enable	N/A		
2	Normal	Forw	Enable	Auto	1000 Full Up
	Enable	Enable	N/A		

Mobility Configuration

Mobility Protocol Port..... 16666
Mobility Security Mode.....


```

Disabled
Default Mobility Domain.....
airespacerf
Mobility Group members configured..... 3

Switches configured in the Mobility Group
MAC Address          IP Address          Group Name
00:0b:85:33:a8:40    192.168.5.70       <local>
00:0b:85:40:cf:a0    192.168.120.100    <local>
00:0b:85:43:8c:80    192.168.5.40       airespacerf

Interface Configuration
Interface Name..... ap-
manager
IP Address.....
192.168.120.101
IP Netmask.....
255.255.255.0
IP Gateway.....
192.168.120.1
VLAN.....
untagged
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port.....
Unconfigured
Primary DHCP Server.....
192.168.1.20
Secondary DHCP Server.....
Unconfigured
ACL.....
Unconfigured
AP Manager..... Yes

Interface Name.....
management
MAC Address.....
00:0b:85:40:cf:a0
IP Address.....
192.168.120.100
IP Netmask.....
255.255.255.0
IP Gateway.....
192.168.120.1
VLAN.....
untagged
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port.....
Unconfigured
Primary DHCP Server.....
192.168.1.20
Secondary DHCP Server.....
Unconfigured
ACL.....
Unconfigured
AP Manager..... No

Interface Name.....
service-port
MAC Address.....
00:0b:85:40:cf:a1
IP Address.....
192.168.250.100

```

```

IP Netmask.....
255.255.255.0
DHCP Protocol.....
Disabled
AP Manager..... No

Interface Name.....
virtual
IP Address.....
1.1.1.1
Virtual DNS Host Name.....
Disabled
AP Manager..... No

WLAN Configuration

WLAN Identifier..... 1
Network Name (SSID).....
lab120wlc4402ip100
Status.....
Enabled
MAC Filtering.....
Enabled
Broadcast SSID.....
Enabled
AAA Policy Override.....
Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60
seconds
Session Timeout..... 1800
seconds
Interface.....
management
WLAN ACL.....
unconfigured
DHCP Server.....
Default
Quality of Service..... Silver
(best effort)
WMM.....
Disabled
802.11e.....
Disabled
Dot11-Phone Mode (7920).....
Disabled
Wired Protocol..... None
IPv6 Support.....
Disabled
Radio Policy..... All
Radius Servers
  Authentication.....
192.168.1.20 1812
Security

  802.11 Authentication:..... Open
System
  Static WEP Keys.....
Enabled
    Key Index:.....
1
    Encryption:.....
104-bit WEP
  802.1X.....

```

```

Disabled
  Wi-Fi Protected Access (WPA1).....
Disabled
  Wi-Fi Protected Access v2 (WPA2).....
Disabled
  IP Security.....
Disabled
  IP Security Passthru.....
Disabled
  L2TP.....
Disabled
  Web Based Authentication.....
Disabled
  Web-Passthrough.....
Disabled
  Auto Anchor.....
Disabled
  Cranite Passthru.....
Disabled
  Fortress Passthru.....
Disabled

RADIUS Configuration
Vendor Id Backward Compatibility.....
Disabled
Credentials Caching.....
Disabled
Call Station Id Type..... IP
Address
Administrative Authentication via RADIUS.....
Enabled
Keywrap.....
Disabled

Load Balancing Info
Aggressive Load Balancing.....
Enabled
Aggressive Load Balancing Window..... 0
clients

Signature Policy
  Signature Processing.....
Enabled

Spanning Tree Switch Configuration

STP Specification..... IEEE 802.1D
STP Base MAC Address.....
00:0B:85:40:CF:A0
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15

Spanning Tree Port Configuration

STP Port ID..... 8001
STP Port State..... Forwarding
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 4
STP Port Path Cost Mode..... Auto

```

STP Port ID.....	8002
STP Port State.....	Forwarding
STP Port Administrative Mode.....	802.1D
STP Port Priority.....	128
STP Port Path Cost.....	4
STP Port Path Cost Mode.....	Auto

[Overbruggingsparameters voor APs configureren](#)



Deze sectie verschaft instructies over het configureren van de rol van AP in het netwerk van het netwerk en verwante overbruggingsparameters. U kunt deze parameters configureren met behulp van de GUI of de CLI.

1. Klik op **Draadloos** en vervolgens op **Alle APs** onder Access Point. De pagina Alle APs verschijnt.
2. Klik op de koppeling Detail voor uw AP1510 om toegang te krijgen tot de pagina Alle APs > Details

Op deze pagina wordt de AP Mode onder General automatisch ingesteld op Bridge voor AP's met overbruggingsfuncties, zoals AP1510. Deze pagina toont deze informatie ook onder Bridging Informatie. Selecteer onder Overbruggingsinformatie een van deze opties om de rol van deze AP in het netwerk van het netwerk van de mazen te specificeren:

- **meshAP**-Kies deze optie als AP1510 een draadloze verbinding met de controller heeft.
- **RootAP**-Kies deze optie als AP1510 een bekabelde verbinding met de controller heeft.

Bridging Information

AP Role	MeshAP 
Bridge Type	Outdoor
Bridge Group Name	<input type="text"/>
Ethernet Bridging	<input type="checkbox"/>
Backhaul Interface	802.11a
Bridge Data Rate (Mbps)	18 

[Verifiëren](#)

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

Nadat u het APs-register met de WLC hebt geregistreerd, kunt u deze bekijken onder het tabblad Draadloos boven in de GUI van de WLC:

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

All APs

Search by Ethernet MAC

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
lab120br1510ip152	8	00:0b:85:5e:5a:80	Enable	REG	1	Detail Bridging Information
lab120br1510ip150	10	00:0b:85:5e:40:00	Enable	REG	1	Detail Bridging Information

Op het CLI kunt u de opdracht samenvatting van de **show** gebruiken om te verifiëren dat AP's die bij de WLC zijn geregistreerd:

(Cisco Controller) >**show ap summary**

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
lab120br1510ip152	2	OAP1500	00:0b:85:5e:5a:80	default_location	1
lab120br1510ip150	2	OAP1500	00:0b:85:5e:40:00	default_location	1

(Cisco Controller) >

Klik op **Bridging Details** in de GUI om de rol van de AP te verifiëren:

All APs > lab120br1510ip152 > Bridging Details

Bridging Details		Bridging Links	
AP Role	RAP	Parent	
Bridge Group Name		Child	lab120br1510ip150 : 00:0b:85:5e:40:00
Backhaul Interface	802.11a		
Switch Physical Port	1		
Routing State	Maintenance		
Malformed Neighbor Packets	0		
Poor Neighbor SNR reporting	0		
Blacklisted Packets	0		
Insufficient Memory reporting	0		
Rx Neighbor Requests	37		
Rx Neighbor Responses	0		
Tx Neighbor Requests	0		
Tx Neighbor Responses	37		
Parent Changes count	0		
Neighbor Timeouts count	0		
Node Hops	0		

Op het CLI kunt u de opdrachten **<Cisco AP>Show mesh-pad <Cisco AP>** gebruiken en de opdrachten **<Cisco AP>tonen** om te controleren of de AP's die bij de WLC zijn geregistreerd:

```
(Cisco Controller) >show mesh path lab120br1510ip152
00:0B:85:5E:5A:80 is RAP
```

```
(Cisco Controller) >show mesh neigh lab120br1510ip152
```

```
AP MAC : 00:0B:85:5E:40:00
```

```
FLAGS : 160 CHILD
```

```
worstDv 255, Ant 0, channel 0, biters 0, ppiters 10
```

```
Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0
```

```
adjustedEase 0, unadjustedEase 0
```

```
txParent 0, rxParent 0
```

```
poorSnr 0
```

```
lastUpdate 1150103792 (Mon Jun 12 09:16:32 2006)
```

```
parentChange 0
```

```
Per antenna smoothed snr values: 0 0 0 0
```

```
Vector through 00:0B:85:5E:40:00
```

```
(Cisco Controller) >
```

Problemen oplossen

Maasje AP's associëren niet met de WLC is een van de meest voorkomende kwesties die gezien worden in de Mesh-implementatie. Voltooi deze controles:

1. Controleer of het MAC-adres van het access point in de Mac Filter lijst in de WLC is toegevoegd. Dit kan worden gezien onder **Security > Mac Filtering**.
2. Controleer het gedeelde geheim tussen de RAP en de MAP. U kunt dit bericht in de WLC zien wanneer er een fout in de toets zit. "#LWAPP SAMENWERKING-request AUTH_STRING_PAYLOAD, ongeldige BRIDGE-sleutelhash AP 00:0b:85:68:c1:d0" **Opmerking:** Probeer altijd de optie **Configuration Zero Touch** te gebruiken indien deze voor een versie beschikbaar is. Hiermee stelt u de toets voor de mesh-AP's automatisch in en voorkomt u foutieve indelingen.
3. RAP's verzenden geen uitzendberichten op hun radio-interface. Configureer de DHCP-server om IP-adressen door de unicast te verzenden, zodat MAP hun IP-adressen door de RAP kan laten doorsturen. Gebruik anders een statische IP voor de MAP.
4. Laat de naam van de Bridge Group bij standaardwaarden achter of zorg ervoor dat de namen van de Bridge Group exact hetzelfde zijn ingesteld op MAP's en de corresponderende RAP.

Dit zijn kwesties die specifiek zijn voor mesh access points. Voor aansluitingsproblemen die tussen de WLC en een access point gemeenschappelijk zijn, raadpleegt u [Troubleshooter met een lichtgewicht access point dat geen draadloze LAN-controller sluit](#).

Opdrachten voor troubleshooting

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

opdrachten gebruikt.

U kunt deze debug-opdrachten gebruiken om problemen met de WLC op te lossen:

- [debug de status van pem](#); gebruikt om de beheerder van het toegangsbeleid te configureren debug opties.
- [debug pem gebeurtenissen om te zetten](#)-gebruikt om de toegangsbeleidsbeheerder te configureren debug opties.
- [debug dhcp bericht laat](#)-het debug van DHCP-berichten zien die van en naar de DHCP-server worden uitgewisseld.
- [debug DHCP-pakket](#): laat het debug van DHCP-pakketgegevens zien die naar en van de DHCP-server worden verzonden.

Sommige extra **debug**-opdrachten die u kunt gebruiken voor probleemoplossing zijn:

- **debug lwapp fouten maken**—tonen het debug van LWAPP-fouten.
- **debug pm laat toe**-toont het debug van certificaatberichten die tussen AP en WLC worden doorgegeven.

Dit **debug lwapp gebeurtenissen maken** het mogelijk dat WLC-opdrachtoutput toont dat de LAP bij de WLC wordt geregistreerd:

```
(Cisco Controller) >debug lwapp events enable
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 Received LWAPP JOIN REQUEST  
from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1'
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce  
00:0B:85:40:CF:A0 rxNonce 00:0B:85:5E:40:00
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from  
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully added NPU Entry for  
AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101, Switch Port: 12223,  
intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop  
MAC: 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of  
LWAPP Join-Reply to AP 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP  
00:0b:85:5e:40:00 slot 0
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP  
00:0b:85:5e:40:00 slot 1
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE REQUEST  
from AP 00:0b:85:5e:40:00 to 00:0b:85:40:cf:a3
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00  
-- static 1, 192.168.120.150/255.255.255.0, gw 192.168.120.1
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring  
-A regDfromCb -A
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring  
-A regDfromCb -A
```

Mon Jun 12 09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Config-Message to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID 'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID 'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00 associated. Last AP failure was due to Link Failure, reason: STATISTICS_INFO_RES

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 0!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 1!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

[Gerelateerde informatie](#)

- [Invoergids voor Cisco mesh-netwerkoplossing](#)
- [Snelle startgids: Cisco Aironet 1500 Series lichtgewicht mesh access points voor buitengebruik](#)
- [Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.0](#)
- [Draadloze ondersteuningspagina](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)