

# Poortconfiguratie met RLAN's in een CBW-netwerk

## Doel

Het doel van dit artikel is een Remote Local Area Network (RLAN) netwerk te maken en groepen poorten en access points toe te wijzen op een Cisco Business Wireless (CBW) Primair access point (AP).

## Toepasselijke apparaten | Software versie

- 145 AC ([informatieblad](#)) | 10.4.1.0 ([laatste download](#))
- 240 AC ([gegevensblad](#)) | 10.4.1.0 ([laatste download](#))

## Inleiding

CBW AP's zijn op 802.11 a/b/g/n/ac (Wave 2) gebaseerd, met interne antennes. Deze AP's ondersteunen de nieuwste 802.11ac Wave 2 standaard voor hogere prestaties, grotere toegang en hoger-dichtheid netwerken.

De 145AC en 240AC AP's waarnaar in dit artikel wordt verwezen hebben de mogelijkheid om in een traditioneel of vermaasd netwerk te worden gebruikt. Dit artikel gebruikt de apparatuur voor een traditioneel draadloos netwerk.

Als u de grondbeginselen van netwerk van het netwerk wilt leren, controleer dan [Cisco Business: Welkom in draadloze mesh-netwerken](#).

Als u de poortconfiguratie in een netwerk liever doet, lees dan [Configureer Ethernet-poorten van Cisco Business Wireless Access Point in mesh-modus](#).

In een traditioneel draadloos netwerk wordt een RLAN gebruikt voor het authenticeren van bekabelde klanten die de primaire AP gebruiken. Zodra de bekabelde client met succes tot de Primaire AP toetreedt, switches de LAN poorten het verkeer tussen centrale of lokale switchmodi. Het verkeer vanaf de bekabelde client wordt behandeld als draadloos clientverkeer.

RLAN stuurt de authenticatieaanvraag om de bekabelde client te echt te maken. De authenticatie van de bekabelde client in een RLAN is vergelijkbaar met de centrale geauthenticeerde draadloze client.

Als u slechts één Virtual Local Area Network (VLAN) nodig hebt, hoeft u geen LAN te configureren. Eén netwerk wordt standaard op het AP-netwerk geïnstalleerd, Native VLAN 1. Het heeft open security en alle poorten worden standaard aan dit LAN toegewezen.

Als u niet bekend bent met de gebruikte termen, raadpleegt u [Cisco Business: Lijst van termen van nieuwe termen](#).

RLAN's werken niet in een netwerk met een netwerk. Maken is standaard niet ingeschakeld. Tenzij u eerder de AP in de vermaasingsmodus hebt laten draaien, dient u te gaan.


## Configuratiestappen

In dit ingesloten gedeelte worden tips voor beginners gemarkeerd.

## Inloggen

Log in op de webgebruikersinterface (UI) van de primaire AP. Om dit te doen, open een web browser en voer <https://ciscobusiness.cisco> in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer uw aanmeldingsgegevens in. U kunt ook toegang krijgen tot de primaire AP door [https://\[ipaddress\]](https://[ipaddress]) (van de primaire AP) in een webbrowsers in te voeren.

## Tips voor gereedschap

Als u vragen hebt over een veld in de gebruikersinterface, controleert u op een snijpunt dat er als volgt uitziet: 

## Problemen met de locatie van het pictogram Hoofdmenu uitvouwen?

Navigeer naar het menu aan de linkerkant van het scherm, als u de menuknop niet ziet, klik dan

op dit pictogram om het zijbalkmenu te openen. 

## Cisco Business-app

Deze apparaten hebben metgezelapps die bepaalde beheerfuncties delen met de webgebruikersinterface. Niet alle functies in de gebruikersinterface van het web zijn in de app beschikbaar.

[iOS-app downloaden](#) [Android-app downloaden](#)

## Veelgestelde vragen

Als u nog steeds onbeantwoorde vragen hebt, kunt u ons vaak gestelde vragen document controleren. [FAQ](#)

## Stap 1

Stel het toegangspunt in als het niet al aan is. Controleer de status van het indicatielampje. Wanneer het LED-licht groen knippert, gaat u naar de volgende stap.

Het opstarten van het toegangspunt duurt ongeveer 8 tot 10 minuten. De LED knippert groen in meerdere patronen, wisselend snel door groen, rood en amber voordat hij weer groen wordt. Er kunnen kleine verschillen zijn in de LED-kleurintensiteit en -tint.

## Stap 2

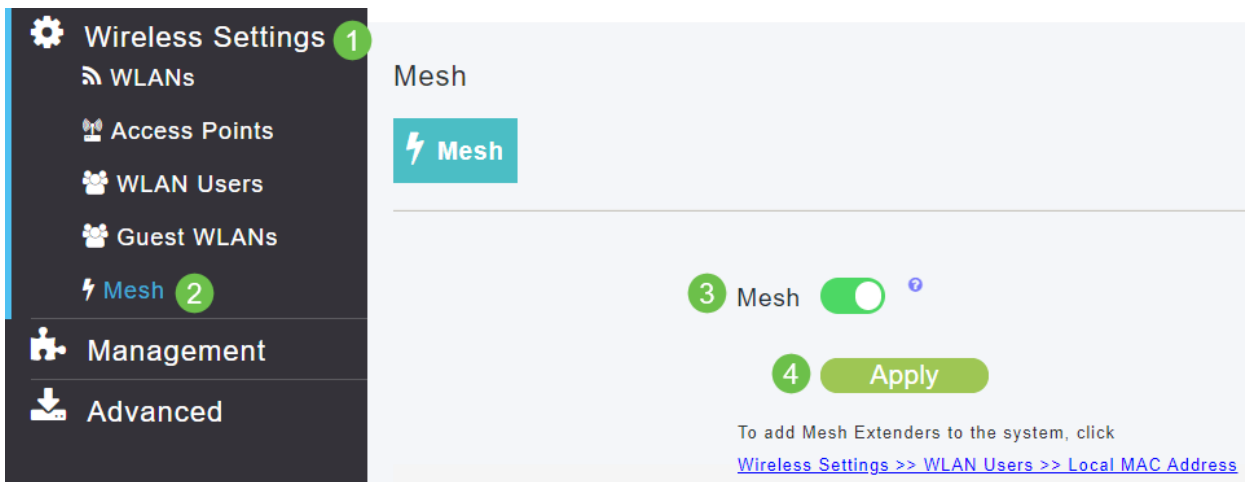
Log in op de webgebruikersinterface (UI) van de primaire AP. Open een webbrowsers en voer <https://ciscobusiness.cisco> in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer je geloofsbrieven in.

U kunt het ook benaderen door het IP-adres van de primaire AP in een webbrowsers in te voeren.

## Stap 3

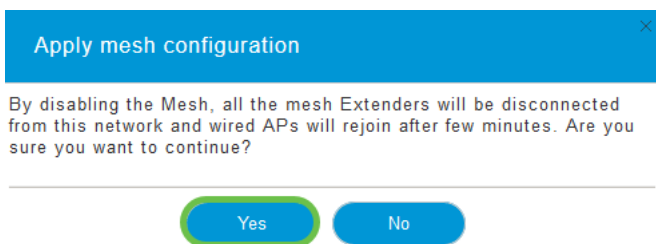
AP kan niet in maaswijdtefunctie zijn voor een RLAN om te werken. Als u de vermakingsmodus

wilt uitschakelen, navigeer dan naar **Draadloze instellingen > mesh**. Selecteer deze optie om het netwerk uit te schakelen. Als uw AP nieuw is of u weet dat de maasmodus niet aan is, kunt u naar [Stap 7](#) overgaan.



## Stap 4

Bevestig dat u de maasmodus wilt uitschakelen door op **Ja** te klikken.



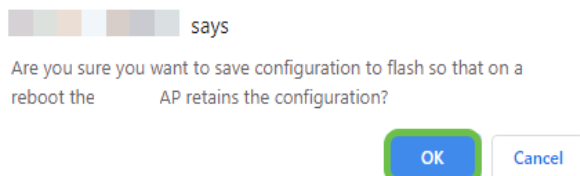
## Stap 5

Vergeet niet uw configuraties op te slaan door op het pictogram **Opslaan** in het rechter bovenpaneel van het Web UI-scherm te klikken.



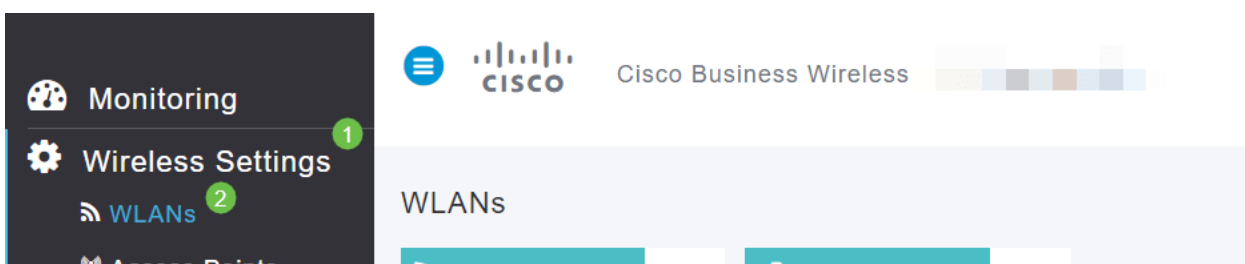
## Stap 6

Bevestig de Opslaan door op **OK** te klikken. Het AP zal opnieuw beginnen. Dit duurt 8 tot 10 minuten.



## Stap 7

Een LAN kan worden gemaakt door in te schakelen op **draadloze instellingen > WLAN's**. Selecteer vervolgens **Nieuwe WLAN/LAN toevoegen**.



## Stap 8

Selecteer **RLAN**. Maak een naam voor het profiel.

Add new WLAN/RLAN ✕

General **RLAN Security** VLAN & Firewall Traffic Shaping

---

Network ID

Type  **1**

Profile Name \*  **2**

Enable

---

## Stap 9 (Gebruik Open Security)

Onder het tabblad *LAN-beveiliging*. U kunt onder *Type beveiliging* de optie *Openen* of *802.1x* selecteren.

In dit voorbeeld werd het *Type Beveiliging* standaard ingeschakeld.

Klik op **Apply** (Toepassen). Dit programma wordt automatisch geactiveerd. Naar [Stap 11](#).

Edit RLAN ✕

General **RLAN Security** VLAN & Firewall Traffic Shaping

---

Guest Network

MAC Filtering  ?

Security Type  **1**

---

**2**

## Stap 10a (met 802.1x security)

Voor het instellen van Externe Straal moet u een Radius Server hebben die in *Admin Account* onder *RADIUS* is ingesteld in *Expert View*. Klik op het **pijl** in het bovenste menu van het web UI om te switches naar *Expert View*. Zie [Straal voor](#) meer informatie over het instellen van een RADIUS-server



## Stap 10b (met 802.1x security)

Als u 802.1X voor het security type kiest, moeten er meer opties worden geselecteerd. U dient het volgende te selecteren:

- *Host Mode - Single Host of Multi-Host*

- *Verificatieserver - Externe straal of AP*
- *MAB modus - Ingeschakeld of uitgeschakeld* Om MAC-adressen toe te voegen, volgt u de instructies in de volgende stap.

Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping

Guest Network

MAC Filtering  ?

Security Type 802.1X

Host Mode Single Host 1

Authentication Server External Radius 2

No RADIUS Server is configured for Authentication and Accounting. RADIUS Server can be configured from 'Admin Accounts > RADIUS'(Expert view)

MAB Mode

RADIUS Server

Add RADIUS Authentication Server 3

State	Server IP Address	Port

## Stap 11 (optioneel)

De modus MAC Verificatie Bypass (MAB) betekent dat als u een MAC-adres hebt dat vermeld staat onder WLAN-gebruikers, het apparaat niet hoeft te authenticeren. De vermelde MAC-adressen kunnen de authenticatie omzeilen die ofwel automatisch toegang tot het netwerk krijgt ofwel automatisch ontkend wordt. Dit zou handig zijn in een geval waar een IP-telefoon op een PoE poort op een switch is aangesloten.

U kunt elk MAC-adres op twee manieren labelen:

1. *Toegestaan* - Het apparaat krijgt automatische toegang.
2. *Blocklisted* - Het apparaat wordt automatisch de toegang geweigerd.

Monitoring

Wireless Settings 1

WLANs

Access Points

WLAN Users 2

Guest WLANs

Mesh

Management

Advanced

Cisco Business Wireless 145AC Access Point

WLAN Users

Users 1

WLAN Users Local MAC Addresses ?

Search ?

+ Add MAC Address Refresh

Number of Blocklist:0 Number of Allowlist:3

Action	MAC Address	Type	Profile Name	Description
3	a4: : :20	Allowlist	Any WLAN/RLAN	CBW145AC-0b20
	4c: : :68	Allowlist	Any WLAN/RLAN	CBW141ACM-7468
	4c: : :1	Allowlist	Any WLAN/RLAN	CBW140AC-cba1

## Stap 12

Onder het tabblad *VLAN & Firewall* kunt u selecteren om *VLAN*-markering te gebruiken en een *VLAN-ID*-nummer te selecteren.

Client IP Management

Use VLAN Tagging  **1**

VLAN ID \*  **2**

Enable Firewall

VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN

## Stap 13 (optioneel)

U kunt **Firewall inschakelen** als u *toegangscontrolelijsten (ACL's)* wilt configureren, zodat u toegang voor specifieke IP-adressen of VLAN's kunt toestaan of afwijzen. Dit wordt gebruikt als iemand in het netwerk poortapparaat is aangesloten om verbinding te maken met het netwerk.

Client IP Management

Use VLAN Tagging

VLAN ID \*

Enable Firewall  **1**

**WLAN Post-auth ACL**

ACL Name(IPv4)

ACL Name(IPv6)

**VLAN ACL**

ACL Name(IPv4)

ACL Direction

## Stap 14 (optioneel)

Onder het tabblad *Traffic Shaping* kunt u traffic shaping configureren door **Application Visibility Control** in te schakelen. Dit stelt prioritering van verkeer in.

Application Visibility Control  **1**

AVC Profile

**2**

Action	S.L No.	Application	Action
--------	---------	-------------	--------

## Stap 15 (optioneel)

Onder het tabblad *Scheduling* kunt u een programma instellen. Dit stelt de tijden in dat de poort kan worden aangesloten op het netwerk.

Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping **Scheduling**

Schedule WLAN **No Schedule**

When 'No Schedule' is selected, all the below scheduling information would be cleared.

Apply to all weekdays

Day	Availability	From	To	Timeline
Monday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Tuesday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Wednesday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Thursday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Friday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Saturday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Sunday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24

## Stap 16 (optioneel)

Nu het netwerk is gemaakt, kunt u navigeren naar **Draadloze instellingen > Toegangsgroepen**. Hier kunt u groepen toevoegen of bewerken. Om dit scherm te bekijken, moet u in *Expert View* zitten, die u in [Stap 10a](#) hebt geselecteerd.

Wireless Settings 1

WLANs

Access Points

Access Points Groups 2

WLAN Users

Guest WLANs

Mesh

Management

Services

Advanced

Access Points Groups

1

Add new group Refresh

Action AP Group name

Warehouse

default-group

1 1 10

Add new group

General WLANs Access Points RF Profile Ports

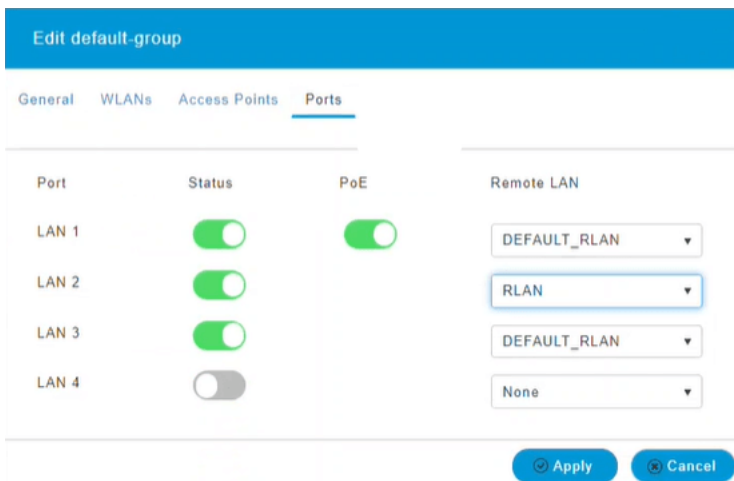
3 AP Group name Warehouse

AP Group description

Apply Cancel

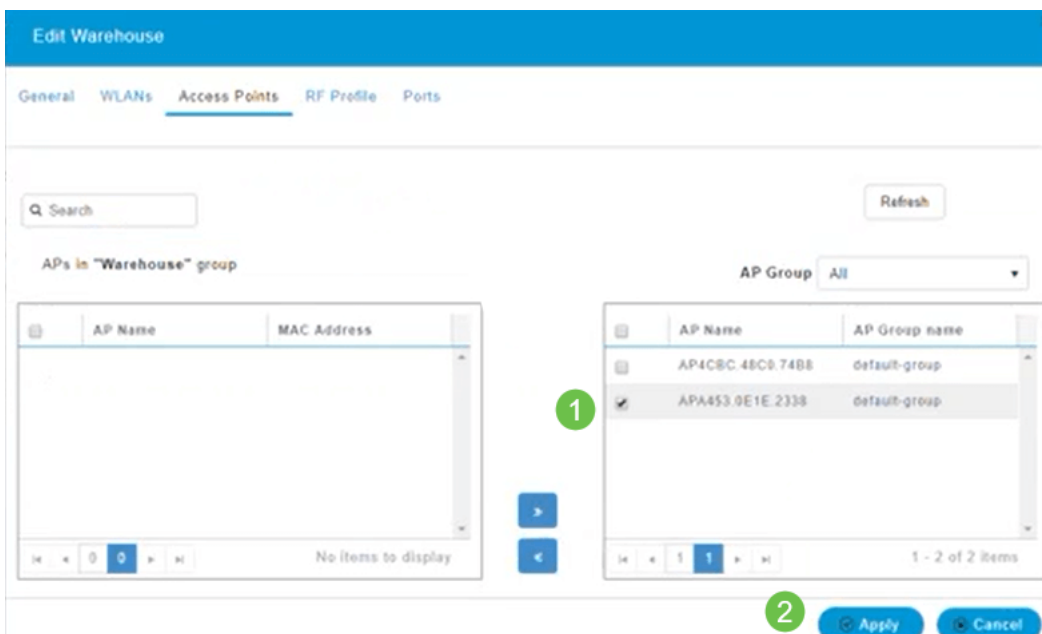
## Stap 17

Onder het tabblad *Port* kunt u de poorten op het AP toewijzen aan specifieke externe LAN's.



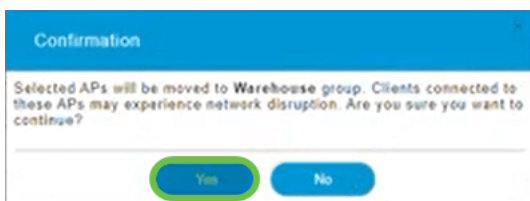
## Stap 18

Onder het tabblad *Access Point*, moet u een bepaald access point aan die Access Point Group toewijzen. Klik op **Apply** (Toepassen).



## Stap 19

Selecteer **Ja** om te bevestigen.



## Stap 20

Vergeet niet uw configuraties op te slaan door op het pictogram **Opslaan** in het rechter bovenpaneel van het Web UI-scherm te klikken.



## Stap 21

Bevestig de Opslaan door op **OK** te klikken. Het AP zal opnieuw beginnen. Dit duurt 8 tot 10



minuten.

 says

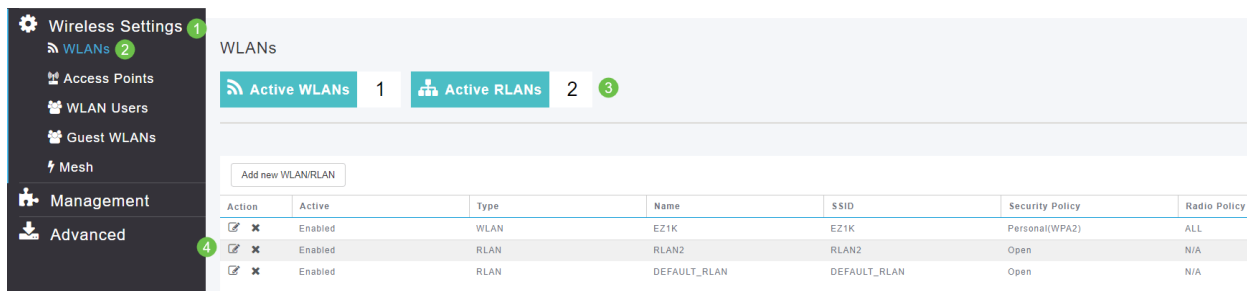
Are you sure you want to save configuration to flash so that on a reboot the AP retains the configuration?

OK

Cancel

## Bekijk het netwerk

Als u het netwerk wilt bekijken dat u hebt gemaakt, selecteert u **Draadloze instellingen > WLAN's**. U ziet het aantal actieve LAN's verhoogd naar 2 en het nieuwe netwerk wordt weergegeven.



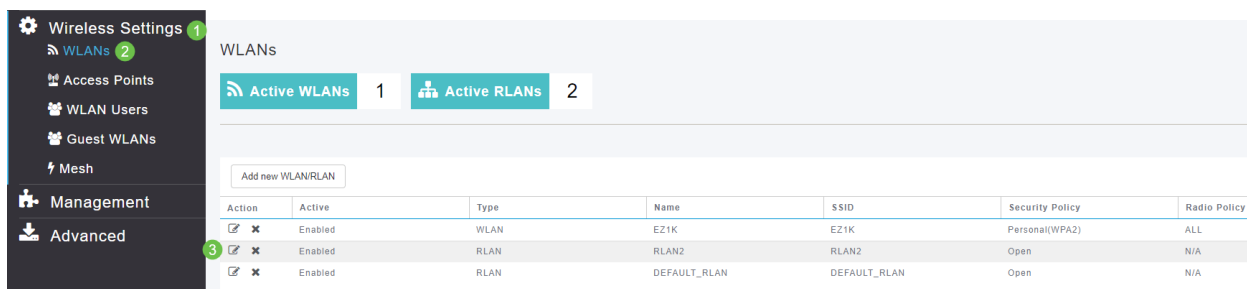
Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/>	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL
<input checked="" type="checkbox"/>	Enabled	RLAN	RLAN2	RLAN2	Open	N/A
<input checked="" type="checkbox"/>	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A

## Het netwerk bewerken

Wanneer u op **Toepassen** hebt geklikt aan het eind van het installatie van uw netwerk, wordt het netwerk automatisch geactiveerd. Als u ooit het netwerk uit moet schakelen of andere wijzigingen wilt aanbrengen, volgt u de onderstaande eenvoudige stappen.

### Stap 1

Selecteer **Draadloze instellingen > WLAN's**. Klik op het pictogram **Bewerken**.



Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/>	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL
<input checked="" type="checkbox"/>	Enabled	RLAN	RLAN2	RLAN2	Open	N/A
<input checked="" type="checkbox"/>	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A

### Stap 2

U ontvangt een pop-up-melding als u weet dat het bewerken van het netwerk tijdelijk wordt onderbroken. Bevestig dat u wilt doorgaan door op **Ja** te klikken.

Edit RLAN

RLAN is in enable state. Editing the RLAN configuration will disrupt the network momentarily. Do you want to continue.?

Yes

No

### Stap 3 (Inschakelen/uitschakelen)

In het venster **WLAN/LAN bewerken** selecteert u onder **Algemeen** de optie **Ingeschakeld** of **uitgeschakeld** om het netwerk in/uit te schakelen. Klik op **Apply** (Toepassen).

General | RLAN Security | VLAN & Firewall | Traffic Shaping

Network ID: 3

Type: RLAN

Profile Name \*: RLAN2

Enable:  1

2 Apply Cancel

## Stap 4 (Andere instellingen bewerken)

Navigeer naar de tabbladen *RLAN Security*, *VLAN & Firewall* of *Traffic Shaping* als u instellingen moet wijzigen. Klik op **Toepassen** zodra u wijzigingen hebt aangebracht.

Edit RLAN

General | RLAN Security | VLAN & Firewall | Traffic Shaping

1

Guest Network:

MAC Filtering:  ?

Security Type: Open

2 Apply Cancel

## Stap 5

Vergeet niet uw configuraties op te slaan door op het pictogram **Opslaan** in het rechter bovenpaneel van het Web UI-scherm te klikken.



## Conclusie

U hebt nu een netwerk van RLAN op uw CBW netwerk gemaakt. Geniet ervan en voel zich vrij er meer aan toe te voegen als het in je behoeften past.

[Veelgestelde vragen](#) [Straal upgrade van firmware](#) [RLAN's Toepassingsprofielen](#) [Clientprofielen](#) [Primaire AP-tools](#) [Umbrella](#) [WLAN-gebruikers](#) [Vastlegging traffic shaping](#) [Rogues](#) [Interferiers](#) [Configuratie-beheer](#) [mesh-poortconfiguratie](#) [Welkom bij CBW mesh-netwerken](#) [Guest Network met e-mailverificatie en RADIUS-accounting](#) [Probleemoplossing](#) [Een Draytek-router met CBW gebruiken](#)