# WGB-roaming: Interne details en configuratie

## Inhoud



## Inleiding

Cisco Workgroup Bridge (WGB) is een zeer nuttig gereedschap voor het ontwerp en de implementatie van een draadloos netwerk, omdat het niet-draadloze apparaten in staat stelt mobiliteit te verkrijgen. WGB geeft veel details over roaming, toegang tot beveiliging, enzovoort, die inzetscenario's beïnvloeden afhankelijk van uw behoeften.

In codeversies 12.4(25d)JA en later, introduceerde Cisco een reeks opdrachten en wijzigingen om het gebruik van WGB op hogesnelheids-roaming-omgevingen te optimaliseren.

Dit document behandelt verschillende aspecten van de manier waarop een WGB werkt, waaronder de beslissingspunten voor roaming-algoritmen, en de manier waarop zij dit voor het beoogde gebruiksmodel moet configureren.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze LAN-oplossing
- Cisco-werkgroepbridge

## Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

# Wat is een werkgroepbrug?

Een WGB is in principe een access point (AP) dat is geconfigureerd om te fungeren als draadloze client voor een infrastructuur en om Layer 2 connectiviteit te bieden voor de apparaten die zijn aangesloten op zijn Ethernet-interface.

Een typische WGB-toepassing heeft deze componenten:

- WGB-apparaat, normaal gesproken met ten minste één radio- en één Ethernet-interface
- Een draadloze infrastructuur, die gewoonlijk root AP wordt genoemd, die ofwel Autonoom of Unified kan zijn.
- Een of meer bekabelde clientapparaten aangesloten op de WGB. Dit document heeft geen betrekking op scenario's met een gemengde rol (één radio als WGB, één radio als wortel op dezelfde AP).

Er zijn drie hoofdtypes van WGB:

- **Cisco WGB**: Cisco WGB is elke op Cisco IOS® gebaseerde AP die is geconfigureerd als WGB (1130, 1240, 1250, enz.). In deze modus wordt het IAPP-protocol gebruikt om de netwerkinfrastructuur te informeren over de apparaten die de WGB op zijn Ethernet-interface heeft geleerd. In dit geval heeft de Wireless LAN Controller (WLC) of root AP Layer 2 zichtbaarheid van de apparaten die worden opgehangen vanaf de WGB.

- **Niet Cisco WGB:** Dit is een apparaat van een derde dat als WGB handelt, dat een of meer aangesloten apparaten op de draadloze infrastructuur aansluit. Deze ondersteunen IAPP niet en staan slechts één aangesloten apparaat toe, of voorzien een MAC-adresvertaalmechanisme, dat al hun bekabelde klanten achter één 802.11 MAC-adres verbergt. Deze typen apparaten hebben een speciale behandeling nodig voor adresresolutie Protocol (ARP) en DHCP-frames als de infrastructuur een WLC is vanwege de beveiligingscontroles en de verwerking van frame op controllers.
- **Cisco AP ingesteld als "Universal WGB"**: Dit is een modus die het IAPP-mechanisme onderdrukt, zodat de WGB naar een Cisco-infrastructuur of naar een AP-stam van derden kan worden gebruikt. In dit geval neemt WGB het adres van zijn Ethernet-cliënt en beperkt het aantal apparaten achter zich tot één.

De volgende sectie concentreert zich op het scenario van een WGB van Cisco die of naar autonome of WLC infrastructuur wordt gebruikt.

## Gebruiksscenario's

De meeste WGB-gebruikvoorbeelden zijn:

- Een bekabelde printer aan het netwerk aansluiten
- Verschillende productieimplementaties, waar het niet mogelijk of praktisch is een kabel naar het bekabelde apparaat te laten lopen
- Invoertrajecten, waarbij de WGB aansluitingen biedt van een auto, metro, enz. naar een draadloos netwerk voor buitengebruik
- Draadloze camera's

Elk voorbeeld heeft zijn eigen eisen op het gebied van:

- Bandbreedte nodig om de toepassing te ondersteunen die bovenop de draadloze infrastructuur draait
- Verdraagzaamheid voor roaming-vertraging - Hoe lang duurt het voor de WGB om van huidige AP naar volgende over te gaan terwijl het apparaat beweegt?
- Doorsturen van tijdtolerantie - Hoeveel frames zijn er verloren bij elke roaming?

Een printer gaat niet veel verder, dus zijn de roamingeisen lager. Een trein op WGB daarentegen heeft een fijnafstemming op de roamingcomponent nodig om ervoor te zorgen dat het gedrag tijdens het rijden correct is.

Een videostream kan een grote bandbreedte-eis hebben, dus hij heeft hoge draadloze gegevenssnelheden nodig. Echter, een telemetrie toepassing zou slechts een paar frames van tijd tot tijd nodig kunnen hebben.

Het is van belang dat de eisen vanaf het begin correct worden gedefinieerd, aangezien zij niet alleen van invloed zijn op de configuratie van de WGB, maar ook op de wijze waarop de draadloze infrastructuur moet worden ontworpen. Bijvoorbeeld AP-plaatsing, afstand, energieniveaus, enabled tarieven, enz. hebben allemaal invloed op roamingkenmerken. Daarom zijn alle zaken van cruciaal belang als er behoefte is aan snelle roaming.

Over het algemeen moet je deze details kennen:

- Wat is de benodigde bandbreedte voor de toepassing?
- Wat is de tolerantie voor roaming-vertragingen?

- Kan de toepassing netverbindingen goed afhandelen? Is er een aanvullend reservemechanisme?
- Kan de toepassing pakketverlies goed verwerken? (Zelfs bij het beste draadloze ontwerp moet u een percentage pakketverlies verwachten.)

Dit document gaat niet in op de details over het ontwerpen van een RF-omgeving voor snelle roaming/buitengebruik. Raadpleeg de handleiding voor mesh-communicatie voor buitengebruik.

# Roaming

Bij een draadloos apparaat is roaming een zeer belangrijk onderdeel van zijn functionaliteit.

Raming betekent de mogelijkheid om van de ene AP naar de andere te gaan, beide tot dezelfde draadloze infrastructuur.

Aangezien roaming een verandering nodig heeft van het huidige AP naar het volgende, is er een ontkoppeling of tijd zonder service. Deze verbinding kan klein zijn. Bijvoorbeeld, minder dan 200ms op spraakimplementaties of veel langer, zelfs seconden, als de beveiliging nodig is om een volledige authenticatie op elke rotatiegebeurtenis af te dwingen.

Roaming is nodig zodat het apparaat een nieuwe ouder met hopelijk beter signaal kan vinden, en het kan de netwerkinfrastructuur goed blijven benaderen. Tegelijkertijd kunnen te veel roams meerdere disconnecties of tijd zonder service veroorzaken, wat de toegang beïnvloedt. Het is belangrijk voor een mobiel apparaat, zoals een WGB, om een goed roaming-algoritme te hebben met voldoende configuratiemogelijkheden om zich aan te passen aan verschillende RF-omgevingen en gegevensbehoeften.

## Elementen van roaming

- **triggers:** Elke client implementatie heeft een of meer triggers of gebeurtenissen, die wanneer voldaan aan, het apparaat veroorzaakt om naar een andere ouder AP te bewegen. Voorbeelden: verlies van een baken (apparaat hoort niet meer de regelmatige beakens van AP), pakketreizen, signaalniveau, geen ontvangen gegevens, ontvangen verificatiekader, lage gegevenssnelheid in gebruik, enz. De mogelijke triggers kunnen verschillen van de uitvoering van de cliënt op een andere omdat ze niet volledig gestandaardiseerd zijn. Eenvoudige apparaten kunnen een slechte trigger hebben, wat slechte (kleverige klanten) of onnodige files veroorzaakt. De WGB ondersteunt alle eerdere elementen die zijn beschreven.
- **Scantijd:** Het draadloze apparaat (WGB) besteedt enige tijd aan het zoeken naar potentiële ouders. Dit impliceert normaal gesproken dat je op verschillende kanalen moet gaan, actief of passief naar AP's moet luisteren. Aangezien de radio moet scannen, betekent dit dat de WGB tijd besteedt aan iets anders dan het doorsturen van gegevens. Vanaf deze scantijd kan de WGB een geldige set ouders opbouwen waaraan u kunt roamen.
- **Ouderselectie:** Na een scantijd kan de WGB de potentiële ouders controleren, de beste selecteren en het associatie/authenticatieproces activeren. Soms kan het beslissend zijn om op het huidige moederbedrijf te blijven als er geen aanzienlijk voordeel is bij een roamingevenement (vergeet niet dat roaming te veel kan zijn).
- **Associatie/verificatie:** De WGB-opbrengsten om te associëren aan de nieuwe AP, die normaal zowel 802.11 verificatie- als associatiefase bestrijkt, plus het voltooien van het beveiligingsbeleid dat op de SSID is ingesteld (WAP 2-PSK, CCKM, geen, enz.).

- **Terugzetten doorsturen:** De WGB actualiseert de netwerkinfrastructuur van haar bekende klanten door middel van IAPP-updates na roaming. Na dit punt hervat het verkeer naar/van de verbonden klanten aan het netwerk.

## Configuratiehandleiding - Beveiligingsbeleid

Een belangrijk aspect voor roaming op mobiele apparaten is het beveiligingsbeleid dat op de infrastructuur zal worden toegepast. Er zijn verschillende opties, ieder met goede/slechte punten. Dit zijn de belangrijkste:

- **Openen** — Deze hebben geen beveiliging. Dit is het snelste en eenvoudigste van al het beleid. Dit is het belangrijkste probleem dat de ongeoorloofde toegang tot de infrastructuur niet wordt beperkt en geen bescherming tegen aanvallen, waardoor het gebruik ervan wordt beperkt tot zeer specifieke scenario's. Bijvoorbeeld mijnen waar geen externe aanvallen mogelijk zijn door de aard van de inzet.
- **MAC-adresverificatie**—Basiliciteitsniveau gelijk aan open, omdat MAC-adresspoofing een triviale aanval is. Niet aanbevolen vanwege de extra tijd om de MAC-validering te voltooien, waardoor roaming wordt vertraagd.
- **WAP2-PSK**-Biedt een goed coderingsniveau (AES-CCMP), maar de authenticatiebeveiliging hangt af van de kwaliteit van de preShared key. Voor beveiligingsmaatregelen wordt een wachtwoord van minimaal 12 tekens en willekeurig wachtwoord aanbevolen. Overeenkomstig met de vooraf gedeelde sleutelmethode, omdat de toets op meerdere apparaten wordt gebruikt, moet, als de toets wordt ingedrukt, het wachtwoord voor alle apparatuur worden gewijzigd. De roamingsnelheid is acceptabel, omdat deze wordt uitgevoerd in 6 frame-uitwisselingen, en u kunt berekenen wat de bovenste/onderste tijdgrenzen voor de roaming zullen zijn, omdat er geen externe apparatuur bij betrokken is (geen RADIUS-server, enzovoort). In het algemeen is deze methode de meest geschikte na het in evenwicht brengen van problemen en voordelen.
- **WAP2 met 802.1x** - Dit verbetert op de vorige methode door gebruik te maken van een apparaat/gebruikersinterface, dat afzonderlijk kan worden gewijzigd. Het belangrijkste probleem is dat voor roaming deze methode niet goed werkt wanneer het apparaat snel beweegt, of wanneer er korte roamingtijden nodig zijn. In het algemeen wordt gebruik gemaakt van dezelfde zes frames plus de MAP-beurs, die tussen 4 en hoger kunnen liggen. Dit hangt af van het type MAP dat wordt geselecteerd en de grootte van de certificaten. Normaal genomen duurt dit tussen 10 en 20 frames plus de extra vertraging van de verwerking van de Straal Server.
- **WAP2+CCKM**-Dit mechanisme biedt goede bescherming, gebruikt 802.1x om de eerste authenticatie op te bouwen, dan vereist een snelle uitwisseling van slechts 2 frames op elke rand gebeurtenis. Dit biedt een zeer snelle roamingtijd. Het belangrijkste probleem is dat in het geval van een mislukt roam, dit weer terugkeert op 802.1x. Begin dan opnieuw CCKM te gebruiken nadat het echt is geworden. Als de toepassing bovenop de WGB een tijdelijke lange roamingtijd kan tolereren in geval van problemen, kan deze worden gebruikt als de beste optie in plaats van PSK.

Dit document heeft geen betrekking op technologieën die niet zijn aanbevolen, zoals LEAP, WAP-TKIP, EVN, enz.

### WAP2-PSK configureren

Op de WGB, is dit vrij eenvoudig te configureren. U hebt SSID definitie en de juiste encryptie op de radio nodig.

```
dot11 ssid wgbpsk
vlan 32
authentication open
authentication key-management wpa version 2
wpa-psk ascii YourReallySecurePSK!
no ids mfp client

interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

Uw naam van SSID en de vooraf gedeelde sleutel moeten uw netwerkinfrastructuur aanpassen.

## WAP2 configureren met 802.1x

Het bouwt in wezen voort op de vorige configuratie, met toevoeging van MAP-profielen en authenticatiemethode:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
!--- This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb
!--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

## WAP2 configureren met CCKM

Slechts één stap boven WAP2 met slechts één kleine verandering: gebruik van de CCKM-vlag in de SSID-configuratie. Dit veronderstelt dat het WLAN alleen aan de WLC-zijde voor CCKM is geconfigureerd:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

## Waardering van de gebruikte methode

Een snelle controle van de WGB kan de encryptie en het sleutelbeheer in gebruik rapporteren, bijvoorbeeld in CCKM:

```
wgb-1260#sh dot11 associations al
Address            : 0024.97f2.75a0     Name              : lap1140-etsi-1
IP Address         : 192.168.40.10      Interface         : Dot11Radio 0
Device             : LWAPP-Parent      Software Version : NONE
CCX Version        : 5                  Client MFP        : Off

State              : EAP-Assoc          Parent            : -
SSID               : wlan1
VLAN               : 0
Hops to Infra      : 0                  Association Id    : 1
Tunnel Address     : 0.0.0.0
Key Mgmt type      : CCKM               Encryption        : AES-CCMP

Current Rate       : m7.-               Capability        : WMM ShortHdr ShortSlot
Supported Rates    : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates        : disabled           Bandwidth         : 20 MHz
Signal Strength    : -59  dBm           Connected for     : 72 seconds
Signal to Noise    : 41  dB            Activity Timeout : 8 seconds
Power-save         : Off                Last Activity     : 7 seconds ago
Apsd DE AC(s)      : NONE

Packets Input      : 12064              Packets Output    : 136
Bytes Input        : 2892798            Bytes Output      : 19514
Duplicates Rcvd    : 87                 Data Retries      : 8
Decrypt Failed     : 0                  RTS Retries       : 0
MIC Failed         : 0                  MIC Missing       : 0
Packets Redirected: 0                   Redirect Filtered: 0
```

# Roaming configureren

Op WGB kunt u verschillende parameters wijzigen die het roaming-algoritme beïnvloeden.

## Vermeldingen van pakketten

Standaard geeft WGB een frame 64 keer opnieuw over. Als ACK door een ouder niet juist wordt erkend, gaat deze ervan uit dat ouder niet langer geldig is en start een scan-/roaming-proces. Zie dit als een "async" roaming-trigger omdat het op elk moment kan worden uitgevoerd dat een transmissie mislukt.

De opdracht om dit aan te passen, gaat in de dot11-interface en heeft de volgende opties:

```
packet retries NUM [drop]
```

**Totaal**: Dit is tussen 1 en 128, met een standaard van 64. Een goed aantal voor een snelle roaming-trigger is gewoonlijk 32. Een lager aantal is niet raadzaam voor de meeste RF-omgevingen.

**vallen**: Als dit niet het geval is, begint de WGB een roamingevenement wanneer de maximale herhalingen worden bereikt. Indien aanwezig, start de WGB geen nieuwe roaming en gebruikt zij andere triggers, zoals het verlies van een baken en een signaal.

## RSSI-bewaking

WGB kan een pro-actieve signaalscan voor de huidige ouder uitvoeren en een nieuw roamingsproces starten wanneer het signaal onder een verwacht niveau daalt.

Dit proces heeft twee parameters:

- Een timer, die het controleproces elke X seconden wakker maakt
- RSSI-niveau, dat wordt gebruikt om een roamingproces te starten als het huidige signaal lager is.

Bijvoorbeeld:

```
in d0
mobile station period 4 threshold 75
```

De tijd mag niet lager zijn dan wat de WGB nodig heeft om een authentificatieproces te voltooien teneinde een "roaminglus" in bepaalde omstandigheden te voorkomen of een te agressief roaminggedrag te vermijden. In het algemeen dient te worden getest om na te gaan wat de applicatie nodig heeft.

Voor PSK kan het lager zijn dan in MAP-gebaseerde methoden (standaard 2 en 4 voor zeer agressieve toepassingen).

Het RSSI-niveau wordt uitgedrukt als een positief integer, hoewel het in wezen een normaal dBm gemeten niveau is. U dient een iets hoger aantal te gebruiken dan het minimum dat nodig is om uw gegevenssnelheid goed te laten werken. Bijvoorbeeld, als uw gewenste minimumtarief 6 mbps is, zou een drempelwaarde RSSI van -87 moeten volstaan. Voor een 48 mbps heb je -70 dBm nodig, enz.

**Opmerking:** deze opdracht kan ook een "roaming via dataritmische verandering" op gang brengen, wat te agressief is. Het moet worden gebruikt samen met een minimumtarief voor goede resultaten.

## Minimumgegevenssnelheid

Om te beginnen met 12.4(25d)JA, voegde Cisco een configureerbare parameter toe om te controleren wanneer de WGB een nieuw roaming-evenement moet starten als het huidige gegevenstarief voor ouders onder een bepaalde waarde ligt.

Dit is behulpzaam om te verzekeren dat een gewenste lager gebonden aan snelheid wordt gehouden om video of spraaktoepassingen te ondersteunen.

Voordat deze opdracht beschikbaar was, veroorzaakte de WGB regelmatig een roaming wanneer het tarief lager was dan de vorige keer. Als het tarief lager was dan de vorige X-tijd, begon de WGB in feite een roamingproces. In de blogs zag je deze berichten:

```
*Mar  1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower
data rate
```

Dit is te agressief, en normaal was de enige oplossing om één enkele gegevenssnelheid in zowel WGB als op APs te configureren.

Aanbevolen wordt om deze opdracht altijd te configureren wanneer een opdracht voor een mobiele stationsperiode wordt gebruikt:

```
in d0
mobile station  minimum-rate 2.0
```

Hierdoor wordt het nieuwe roamingproces alleen geactiveerd als het huidige tarief lager is dan de ingestelde waarde. Dit vermindert onnodige ruitingen en maakt het mogelijk om een verwachte rentewaarde te behouden.

**Opmerking:** Het bericht `"moest het gegevenstarief verlagen"` zal naar verwachting zelfs bij deze configuratie voorkomen, net zoals het nu alleen moet worden gezien als WGB minder dan ingesteld was, toen de controletijd van de mobiele stationsperiode werd geactiveerd.

## Scankanalen

De WGB scant alle "landkanalen" terwijl hij een roamingevenement doet. Dit betekent dat, afhankelijk van het radiodomein, je kanalen 1 tot 11 kunt scannen op de 2,4 GHz band, of 1 tot 13.

Elk gescande kanaal heeft enige tijd nodig. Op 802.11bg is dit ongeveer 10 tot 13 ms. Op 802.11a kan het tot 150 ms zijn als kanaal is ingeschakeld (dus niet testen, gewoon passieve scan doen).

Een goede optimalisatie is om de gescande kanalen te beperken tot de kanalen die door de infrastructuur in gebruik worden genomen. Dit is vooral belangrijk op 802.11a, omdat de kanaallijst groot is, en de tijd per kanaal kan lang zijn als DFS in gebruik is.

Er zijn drie punten te nemen bij het ontwerpen van een kanaalplan voor WGB/Roaming:

- Probeer voor de 2,4 GHz-band op 1/6/11 te blijven staan om kanaalinterferentie te minimaliseren. Elk ander kanaalplan met 4, enz. is meestal moeilijk om goed te ontwerpen vanuit RF-oogpunt, zonder dat de interferentie toeneemt.
- Het gebruiken van één kanaalinstelling voor alle AP's is een goed idee vanuit scanstandpunt. Dit is alleen maar zinvol als het totale aantal klanten dat moet worden ondersteund zeer laag is en er geen hoge bandbreedte-eisen zijn. Hiermee wordt de tijd voor radioverwijking uit de scantijd geschrapt. Houd er rekening mee dat weinig omgevingen van deze optie kunnen profiteren, dus gebruik voorzichtig.
- Voor de 5,0 GHz-band, als dit mogelijk is door uw lokale regelgeving, maakt het gebruik van niet-DFS-kanalen (36 tot 48) binnenshuis een snellere scantijd mogelijk, omdat WGB elk actief kan onderzoeken, in plaats van passief luisteren langer.

Het kanaalplan dat voor uw plaatsing wordt gebruikt zou andere vereisten kunnen moeten bevatten. Gebruik de algemene RF-ontwerpaanbevelingen.

Zo configureren u de lijst met scankanalen:

```
in d0
mobile station scan 1 6 11
```

**Opmerking:** Mobiel station verschijnt alleen als je de WGB-rol op de radio gebruikt.

**Opmerking:** Controleer of de WGB-scanlijst overeenkomt met de lijst van het infrastructuurkanaal. Als dat niet het geval is, vindt de WGB uw beschikbare AP's niet.

## Timers configureren

Om te beginnen met 12.4(25a)JA, zijn er verschillende nieuwe opdrachten om de hersteltimer te optimaliseren wanneer er een probleem wordt gevonden. Deze zijn alleen beschikbaar wanneer AP in WGB-modus staat.

```
wgb-1260(config)#workgroup-bridge timeouts ?

  assoc-response  Association Response time-out value
  auth-response   Authentication Response time-out value
  client-add      client-add time-out value
  eap-timeout     EAP Timeout value
  iapp-refresh    IAPP Refresh time-out value
```

In het geval van assoc-respons, auth-response, client-add, deze duiden erop hoe lang de WGB zal wachten tot de ouder AP zal antwoorden, alvorens de AP als dood de dood en de volgende kandidaat te beschouwen. De standaardwaarden zijn 5 seconden, wat voor sommige toepassingen te lang is. De minimale timer is 800 ms en wordt aanbevolen voor de meeste mobiele toepassingen.

In het gemak stelt de WGB een maximumtijd vast om te wachten, totdat het volledige MAP-verificatieproces is voltooid. Dit werkt vanuit een MAP-oogpunt om het proces opnieuw op te starten als de MAP-authenticator niet antwoordt. De standaardwaarde is 60 seconden. Let erop dat u nooit een waarde instelt die lager kan zijn dan de werkelijke tijd die nodig is om een volledige 802.1x-verificatie te voltooien. Normaal gesproken is deze instelling op 2 tot 4 seconden correct voor de meeste implementaties.

Voor iapp-verfrissing genereert de WGB standaard een IAPP bulkupdate naar de parent AP na roaming om de bekende bekabelde klanten te informeren. Er is een tweede hertransmissie na associatie ongeveer 10 seconden later. Met deze timer kan de IAPP-bulk snel opnieuw proberen na associatie om de kans te overwinnen dat de eerste IAPP-update verloren ging door RF of coderingstoetsen die nog niet op de parent AP zijn geïnstalleerd. Voor snelle roaming-scenario's kunnen 100 ms worden gebruikt. Zorg er echter voor dat er een groot aantal WGB in gebruik is. Dit verhoogt aanzienlijk het totale aantal IAPP's dat na elke roaming naar de infrastructuur wordt gestuurd.

Voorbeeld voor agressieve waarden:

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

Deze zijn met succes getest op mobiele WGB-implementatiescenario's.

# Andere WGB-optimalisaties

Er zijn andere kleine wijzigingen die in aanmerking moeten worden genomen voor WGB-implementatiescenario's:

## Radio-gerelateerd

- Verminder **rts** - **rts herprobeert 32**. Dit kan wat RF-tijd besparen op agressieve scenario's. Normaal gesproken is dit niet nodig.
- Type antenne: Indien u één antenne (geen diversiteit) gebruikt, dient u de radio te configureren om de algemene prestaties te verbeteren:

```
antenna transmit right-a
antenna receive right-a
```

Diversiteit van de antenne is wenselijk, maar niet altijd mogelijk bij de fysieke installatie van antennes op het voertuig. Voor roaming is een goede keuze voor antennes cruciaal. Niet minder dan 2 dB kan een groot verschil zijn ten opzichte van de gemiddelde normale roamingtijden.

## Verwante

- Om sommige milliseconden op te slaan, beperkt u het houtlogniveau van de console tot alleen fouten: **logconsole-fouten**. Schakel deze niet volledig uit omdat dit negatieve gevolgen kan hebben voor de roamingprestaties onder bepaalde omstandigheden.
- U kunt het beste telnet of ssh uit het Ethernet-gedeelte gebruiken om uitwerpselen of stammen te verzamelen. Dit heeft een veel lager effect op prestaties in vergelijking met houtkap over console: **het fouilleren van de houtmonitor**.
- De opdracht om te begrijpen wat er gebeurt voor WGB roaming-oogpunt is **debug dot11 dot11 0-sporenuplinks**. Dit heeft een laag effect op de CPU, maar maakt geen andere debug-opties mogelijk, tenzij geïnstrueerd, omdat elke optie de totale roaming-tijd kan verhogen.
- Probeer SNTP wanneer mogelijk te gebruiken. Dit houdt de WGB-tijd op sync, wat bijzonder handig is voor het oplossen van problemen.

## MFP-gebruik

- MFP kan vanuit veiligheidsoogpunt nuttig zijn. Een nadeel is echter dat de WGB bij scenario's voor roaming-storingen geen de-auth-frames van de AP-ouder accepteert om nieuwe roaming op gang te brengen als de encryptiesleutel tussen beide verkeerd is gegaan.
- Bij deze zeldzame mislukkingsscenario's kan de WGB tot 5 seconden duren om een nieuwe scan te activeren, als de huidige ouder met een goed RF-signaal kan worden gehoord. Er is een "catch-all"-detectiemechanisme dat WGB kan activeren als er gedurende die tijd geen geldige gegevensframes worden ontvangen.
- Standaard probeert WGB de client-MFP te gebruiken als de SSID WAP2 AES in gebruik heeft.
- Aanbevolen wordt om client MFP uit te schakelen als er snelle hersteltijden nodig zijn (WGB om te reageren op niet-beschermde uitvalsframes). Dit is een compromis tussen veiligheidsbehoeften en snelle hersteltijden. De beslissing hangt af van wat belangrijker is voor het inzetscenario.

```
dot11 ssid wgbpsk
   no ids mfp client
```

## EAP-TLS op WGB en "klokopslaginterval"

Raadpleeg de synchrone IOS Super klokken en de instelling van de Opslagtijd naar NVRAM sectie van Releaseopmerkingen voor Cisco Aironet access points en bruggen voor Cisco IOS release 12.4(21a)JY.

Houd in gedachten dat als u WGB gebruikt, uWGB nooit een kans krijgt om een snp sync te gebruiken omdat deze doorgaans gekoppeld is aan het aangesloten MAC-adres en uWGB BVI geen netwerktoegang heeft. Daarom wordt in het geval van een uWGB, aanbevolen om een goede kloksync in NVRAM bij implementatie op zijn minst te krijgen. Als het aangesloten

netwerkapparaat de mogelijkheid heeft om een NTP-bron te zijn (zowel als een bijgewerkte client via zijn uWGB-verbinding), dan is het mogelijk om te overwegen om de uWGB sntp sync eraf te zetten als een effectief NTP-reflectiepunt.

## Volledig configuratievoorbeeld

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
!
dot11 syslog
!
!
dot11 ssid wgbpsk
   vlan 32
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 7 060506324F41584B56
   no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
!
antenna transmit right-a
antenna receive right-a
  packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
!
```

```
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
interface BVI1
ip address 192.168.32.67 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip

sntp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

## Debug Analysis

Bij elk probleem dat zich voordoet, is het belangrijk om de uitvoer van de **debug dot11 dot11 0-** opdracht voor **het** optrekken van **sporen** als eerste stap op te nemen. Dit geeft een goed beeld van wat er gebeurt met het roamingproces.

Dit is een voorbeeld van de huidige ouder als kandidaat:

```
 Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength
too low
 Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

Dit is trigger voor een laag signaal dat wordt ontvangen. Het hangt af van de X drempelwaarde Y-opdracht van het mobiele station. Het eerste bericht wordt altijd naar de console gestuurd, het tweede maakt deel uit van de uplink debug-sporen. Het is geen probleem, maar een onderdeel van het normale WGB-proces.

```
 Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

Het Uplink-proces dwingt een zuiveringsbeurt van de radiogateway voordat u een kanaalscan start. Deze stap kan van een paar milliseconden tot een aantal seconden duren afhankelijk van kanaalgebruik en wachtrijdiepte. Data frames worden niet vastgesteld. Spraakframes hebben een tijdvergelijking gemaakt en moeten dus sneller worden ingetrokken. Er kan enige vertraging worden waargenomen in lawaaierige omgevingen.

```
 Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
 Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

Dit is de echte kanaalscan die plaatsvindt. Het parkeert de radio ongeveer 10 tot 13 ms per geconfigureerd kanaal.

```
 Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

Dit is de lijst van ontvangen peilingen. Het eerste nummer is het kanaal, de tweede is microseconden genomen om het te ontvangen.

```
 Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0,
load 0
 Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0,
load 0
```

Feitelijke vergelijking gedaan in deze details:

```
 Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet
```

### Selectie ouders

```
 Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done
 Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0,
 Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed.
```

Dit is het punt waarop de roaming 'voltooid' is. Het verkeer hervat zodra de IAPP-frames door de ouder worden verwerkt.

### Informatie over ouders vergelijken

```
 Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0,
load 3
 Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1,
load 0
```

Daarmee wordt de feitelijk aantal associatie-1 afgedrukt (dus wordt WGB zelf niet in het nummer opgenomen) als de "huidige" AP nog steeds het WGB-signaal is dat wordt gebruikt, en worden er dus nog hoop en lading gegeven.

De vergelijk2 drukt de verschillen af. Daarom is het mogelijk een negatief getal te zien. Als test een hoger aantal dan stroom heeft, ziet u negatief.

Afhankelijk van het huidige aantal associatie, lading, signaalverschil, mobiele drempelwaarde, kan de WGB een nieuw ouder selecteren of niet.

De vergelijking is altijd tussen twee AP's, met geselecteerde AP die de huidige voor volgende iteratie vervangt. Daarom kunnen sommige beslissingen aan RSSI op één lijn worden toegeschreven, of aan andere factoren op de volgende test.

## Gerelateerde informatie

- Hoe u IOS WGB met EAP-TLS-verificatie kunt gebruiken in een Cisco Unified Wireless Network
- Technische ondersteuning en documentatie – Cisco Systems