WGB-Roaming: Interne Details und Konfiguration

Inhalt

Einführung

Die Cisco Workgroup Bridge (WGB) ist ein sehr nützliches Tool für das Design und die Bereitstellung eines Wireless-Netzwerks, da sie Geräten ohne Wireless-Funktion die Mobilität ermöglicht. Die WGB bietet viele Details zu Roaming, Sicherheitszugriff usw., die sich je nach Bedarf auf Bereitstellungsszenarien auswirken.

In den Codeversionen 12.4(25d)JA und höher hat Cisco eine Reihe von Befehlen und Änderungen eingeführt, um die Verwendung von WGB in Hochgeschwindigkeits-Roaming-Umgebungen zu optimieren.

In diesem Dokument werden verschiedene Aspekte der Funktionsweise eines WGB beschrieben, einschließlich Entscheidungskriterien für Roaming-Algorithmen und deren Konfiguration für das beabsichtigte Verwendungsmodell.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Wireless LAN-Lösung
- Cisco Workgroup Bridge

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Was ist eine Arbeitsgruppen-Bridge?

Ein WGB ist im Grunde ein Access Point (AP), der als Wireless-Client für eine Infrastruktur konfiguriert ist und Layer-2-Verbindungen für die Geräte bereitstellt, die mit der Ethernet-Schnittstelle verbunden sind.

Eine typische WGB-Bereitstellung umfasst folgende Komponenten:

- WGB-Gerät, in der Regel mit mindestens einem Funkmodul und einer Ethernet-Schnittstelle
- Eine Wireless-Infrastruktur, normalerweise Root AP genannt, die entweder autonom oder einheitlich sein kann.
- Ein oder mehrere mit dem WGB verbundene Client-Geräte. Dieses Dokument behandelt keine Szenarien mit gemischten Rollen (eine Funkeinheit als WGB, eine Funkeinheit als Root auf demselben AP).

Es gibt drei Haupttypen von WGB:

- **Cisco WGB**: Cisco WGB ist ein beliebiger Cisco IOS®-basierter Access Point, der als WGB

konfiguriert ist (1130, 1240, 1250 usw.). Dieser Modus verwendet das IAPP-Protokoll, um die Netzwerkinfrastruktur über die Geräte zu informieren, die der WGB über seine Ethernet-Schnittstelle gelernt hat. In diesem Fall bietet der Wireless LAN Controller (WLC) oder der Root Access Point eine Layer-2-Transparenz der Geräte, die vom WGB "hängen".

- **WGB anderer Anbieter:** Dies ist ein Gerät eines Drittanbieters, das als WGB fungiert und ein oder mehrere kabelgebundene Geräte mit der Wireless-Infrastruktur verbindet. Diese unterstützen IAPP nicht und ermöglichen entweder nur ein kabelgebundenes Gerät oder stellen einen Übersetzungsmechanismus für MAC-Adressen bereit, der alle kabelgebundenen Clients hinter einer einzigen 802.11-MAC-Adresse verbirgt. Diese Gerätetypen müssen aufgrund der Sicherheitsüberprüfungen und der Frame-Verarbeitung auf Controllern besonders mit ARP- (Address Resolution Protocol) und DHCP-Frames behandelt werden, wenn es sich bei der Infrastruktur um einen WLC handelt.
- **Cisco AP konfiguriert als "Universal WGB"**: Dieser Modus unterdrückt den IAPP-Mechanismus, sodass der WGB für eine Cisco Infrastruktur oder für Root-APs von Drittanbietern verwendet werden kann. In diesem Fall übernimmt das WGB die Adresse seines Ethernet-Clients und beschränkt die Anzahl der Geräte hinter diesem Client auf einen.

Im nächsten Abschnitt geht es um das Szenario eines Cisco WGB, das entweder für eine autonome oder WLC-Infrastruktur verwendet wird.

Verwendungsszenarien

Beispiele für typische WGB-Verwendungen:

- Verbinden eines kabelgebundenen Druckers mit dem Netzwerk
- Verschiedene Fertigungsbereitstellungen, in denen ein Kabel mit dem kabelgebundenen Gerät nicht ausgeführt werden kann
- In-Vehicle-Bereitstellungen, bei denen der WGB Verbindungen zwischen Autos, U-Bahnen usw. und einem Wireless-Netzwerk für Außenbereiche bereitstellt
- Kabelgebundene Kameras

Für jedes Beispiel gelten eigene Anforderungen in Bezug auf:

- Zur Unterstützung der Anwendung, die auf der Wireless-Infrastruktur ausgeführt wird, benötigte Bandbreite
- Toleranz bei Roaming-Verzögerungen - Wie lange dauert es, bis das WGB während der Bewegung des Geräts vom aktuellen Access Point zum nächsten wechselt?
- Toleranz für die Weiterleitungszeit: Wie viele Frames gehen bei jedem Roaming verloren?

Ein Drucker bewegt sich nicht sehr stark, daher sind die Roaming-Anforderungen geringer. Bei einem im WGB installierten Zug muss die Roaming-Komponente genauer angepasst werden, um das korrekte Verhalten während der Fahrt sicherzustellen.

Ein Video-Stream kann eine hohe Bandbreitenanforderung aufweisen, sodass er hohe Wireless-Datenraten benötigt. Eine Telemetrie-Anwendung kann jedoch von Zeit zu Zeit nur wenige Frames benötigen.

Es ist wichtig, dass die Anforderungen von Anfang an genau definiert werden, da sie nicht nur die Konfiguration des WGB betreffen, sondern auch, wie die Wireless-Infrastruktur gestaltet werden muss. Beispielsweise wirken sich die Platzierung von Access Points, die Entfernung, die Leistungsstufen, die aktivierten Übertragungsraten usw. auf die Roaming-Eigenschaften aus.

Daher sind alle ein entscheidender Punkt, wenn Hochgeschwindigkeits-Roaming erforderlich ist.

Im Allgemeinen müssen Sie diese Details kennen:

- Welche Bandbreite wird für die Anwendung benötigt?
- Wie hoch ist die Toleranz für Roaming-Verzögerungen?
- Kann die Anwendung Netzwerkausfälle ordnungsgemäß handhaben? Gibt es einen zusätzlichen Sicherungsmechanismus?
- Kann die Anwendung Paketverluste ordnungsgemäß handhaben? (Selbst beim besten Wireless-Design müssen Sie einen Prozentsatz des Paketverlusts erwarten.)

In diesem Dokument wird nicht näher auf das Design einer Funkumgebung für Hochgeschwindigkeits-Roaming/Außenbereiche eingegangen. Weitere Informationen finden Sie im Outdoor Mesh-Bereitstellungsleitfaden.

Roaming

Für ein Wireless-Gerät ist Roaming ein sehr wichtiger Teil seiner Funktionalität.

Im Prinzip bedeutet Roaming die Möglichkeit, von einem Access Point zu einem anderen zu wechseln, die beide zu derselben Wireless-Infrastruktur gehören.

Da beim Roaming eine Änderung vom aktuellen Access Point zum nächsten erforderlich ist, kann die Verbindung unterbrochen oder der Service nicht in Anspruch genommen werden. Diese Trennung kann gering sein. Beispielsweise weniger als 200 ms bei Sprachanwendungen oder viel länger, sogar Sekunden, wenn die erforderliche Sicherheit eine vollständige Authentifizierung für jedes Roaming-Ereignis erzwingt.

Roaming ist erforderlich, damit das Gerät ein neues übergeordnetes Gerät mit hoffentlich besseren Signalen finden und weiterhin ordnungsgemäß auf die Netzwerkinfrastruktur zugreifen kann. Gleichzeitig können zu viele Roams mehrere Verbindungsunterbrechungen oder eine Zeitüberschreitung ohne Dienst verursachen, was den Zugriff beeinträchtigt. Ein Mobilgerät, z. B. ein WGB, muss über einen guten Roaming-Algorithmus mit genügend Konfigurationsmöglichkeiten verfügen, um sich an unterschiedliche Funkumgebungen und Datenanforderungen anzupassen.

Elemente des Roaming

- **Trigger:** Jede Client-Implementierung verfügt über einen oder mehrere Trigger oder Ereignisse, die das Gerät bei Erreichen des Ziels zum Wechseln zu einem anderen übergeordneten Access Point veranlassen. Beispiele: Beacon-Verlust (Gerät hört nicht mehr die regulären Beacons vom AP), Paketretries, Signalpegel, keine empfangenen Daten, Deauthentifizierungsrahmen erhalten, niedrige verwendete Datenrate usw. Die möglichen Auslöser können sich von Client-Implementierung zu Client-Implementierung unterscheiden, da sie nicht vollständig standardisiert sind. Einfachere Geräte verfügen möglicherweise über einen schlechten Trigger-Satz, der schädliche (klebrige Clients) oder unnötige Roaming verursacht. Der WGB unterstützt alle zuvor beschriebenen Elemente.
- **Prüfungszeit:** Das Wireless-Gerät (WGB) sucht einige Zeit nach potenziellen Eltern. Dazu müssen in der Regel verschiedene Kanäle verwendet werden, aktiv nachforschen oder APs passiv zuhören. Da die Funkeinheit scannen muss, bedeutet dies Zeit, dass das WGB anders

als die Weiterleitung von Daten arbeitet. Ab dieser Prüfzeit kann der WGB eine gültige Gruppe von Eltern erstellen, zu denen ein Roaming möglich ist.
- **Übergeordnete Auswahl:** Nach der Scan-Zeit kann der WGB die potenziellen Eltern überprüfen, den besten auswählen und den Assoziations-/Authentifizierungsprozess auslösen. Manchmal kann der Entscheidungspunkt darin bestehen, im aktuellen übergeordneten Element zu bleiben, wenn ein Roaming-Ereignis keinen wesentlichen Vorteil bietet (denken Sie daran, dass zu viel Roaming schlecht sein kann).
- **Zuordnung/Authentifizierung:** Die WGB wird weiterhin dem neuen Access Point zugeordnet, der normalerweise sowohl die 802.11-Authentifizierungs- und Zuordnungsphasen abdeckt, als auch die auf der SSID konfigurierten Sicherheitsrichtlinien (WPA 2-PSK, CCKM, None usw.) abschließt.
- **Wiederherstellung der Datenverkehrsweiterleitung:** Die WGB aktualisiert die Netzwerkinfrastruktur ihrer bekannten kabelgebundenen Clients nach dem Roaming mithilfe von IAPP-Updates. Danach wird der Datenverkehr zu/von den kabelgebundenen Clients zum Netzwerk fortgesetzt.

Konfigurationsleitfaden - Sicherheitsrichtlinien

Ein wichtiger Aspekt beim Roaming auf Mobilgeräten ist die Sicherheitsrichtlinie, die in der Infrastruktur implementiert wird. Es gibt mehrere Optionen, von denen jede einen guten bzw. schlechten Punkt hat. Dies sind die wichtigsten:

- **Offen** - im Grunde keine Sicherheit. Dies ist die schnellste und einfachste aller Richtlinien. Dies hat das Hauptproblem, nicht den unbefugten Zugriff auf die Infrastruktur zu beschränken, und es besteht kein Schutz vor Angriffen, wodurch die Nutzung auf sehr spezifische Szenarien beschränkt wird. So sind beispielsweise Minen, bei denen aufgrund der schieren Natur der Bereitstellung keine externen Angriffe möglich sind.
- **MAC-Adressenauthentifizierung** - Im Prinzip dieselbe Sicherheitsstufe wie offen, da MAC-Adressen-Spoofing ein trivialer Angriff ist. Wegen der zusätzlichen Zeit zum Abschließen der MAC-Validierung nicht empfohlen, wodurch das Roaming verlangsamt wird.
- **WPA2-PSK**: Bietet eine gute Verschlüsselungsstufe (AES-CCMP), aber die Authentifizierungssicherheit hängt von der Qualität des vorinstallierten Schlüssels ab. Für Sicherheitsmaßnahmen wird ein Kennwort mit mindestens 12 Zeichen und zufällig ausgewählte Zeichen empfohlen. Ähnlich wie bei der Methode des vorinstallierten Schlüssels muss das Kennwort für alle Geräte geändert werden, wenn der Schlüssel auf mehreren Geräten verwendet wird. Die Roaming-Geschwindigkeit ist akzeptabel, wie sie bei 6 Frame-Austauschen erfolgt. Sie können berechnen, welche oberen/unteren Zeitbegrenzungen für den Abschluss des Vorgangs gelten, da es keine externen Geräte (kein RADIUS-Server usw.) umfasst. Im Allgemeinen ist diese Methode nach dem Ausgleich von Problemen und Vorteilen die bevorzugte Methode.
- **WPA2 mit 802.1x**: Diese Methode verbessert die vorherige Methode, indem eine Pro-Gerät-/Benutzer-Anmeldeinformationen verwendet wird, die einzeln geändert werden können. Das Hauptproblem besteht darin, dass diese Methode beim Roaming nicht ordnungsgemäß funktioniert, wenn sich das Gerät schnell bewegt oder kurze Roaming-Zeiten erforderlich sind. Im Allgemeinen werden dabei die gleichen 6 Frames sowie der EAP-Austausch verwendet, der zwischen 4 und höher liegen kann. Dies hängt davon ab, welcher EAP-Typ und welche Zertifikatsgrößen ausgewählt sind. In der Regel dauert dies zwischen 10 und 20 Frames plus

der zusätzlichen Verzögerung der Radius-Server-Verarbeitung.

- **WPA2+CCKM**: Dieser Mechanismus bietet guten Schutz, verwendet 802.1x zum Erstellen der anfänglichen Authentifizierung und führt dann einen schnellen Austausch von nur 2 Frames für jedes Roaming-Ereignis durch. Dies ermöglicht eine sehr schnelle Roaming-Zeit. Das Hauptproblem besteht darin, dass bei einem ausgefallenen Roam 802.1x wieder aktiviert wird. Anschließend wird CCKM nach der Authentifizierung erneut verwendet. Wenn die Anwendung auf dem WGB gelegentlich eine lange Roaming-Zeit tolerieren kann, kann sie als beste Option im Vergleich zu PSK verwendet werden.

Dieses Dokument behandelt nicht empfohlene Technologien mit Sicherheitsproblemen wie LEAP, WPA-TKIP, WEP usw.

Konfigurieren von WPA2-PSK

Auf dem WGB ist dies relativ einfach zu konfigurieren. Sie benötigen die SSID-Definition und die entsprechende Verschlüsselung im Funk.

```
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
```

Ihr SSID-Name und der Pre-Shared Key müssen mit Ihrer Netzwerkinfrastruktur übereinstimmen.

Konfigurieren von WPA2 mit 802.1x

Sie baut im Wesentlichen auf der vorherigen Konfiguration auf, wobei EAP-Profile und die Authentifizierungsmethode hinzugefügt werden:

```
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
```

Konfigurieren von WPA2 mit CCKM

Nur ein Schritt über WPA2 mit nur einer geringfügigen Änderung: Verwenden des CCKM-Flags in der SSID-Konfiguration. Es wird davon ausgegangen, dass das WLAN nur auf der WLC-Seite für CCKM konfiguriert ist:

```
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
```

Validierung der verwendeten Methode

Eine schnelle Überprüfung des WGB kann die verwendete Verschlüsselung und Schlüsselverwaltung melden, z. B. 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
```

Konfigurieren von Roaming

Auf dem WGB können Sie mehrere Parameter ändern, die sich auf den Roaming-Algorithmus auswirken.

Wiederholungen von Paketen

Standardmäßig überträgt das WGB einen Frame 64-mal erneut. Wenn sie von einem übergeordneten Element nicht ordnungsgemäß bestätigt wird (ACK), wird davon ausgegangen, dass das übergeordnete Element nicht mehr gültig ist, und es wird ein Scan-/Roaming-Prozess gestartet. Betrachten Sie diesen als asynchronen Roaming-Trigger, da er jederzeit bei einem Übertragungsfehler ausgeführt werden kann.

Der Befehl zum Konfigurieren dieses Befehls geht in die Dot11-Schnittstelle, und er umfasst die folgenden Optionen:

```
packet retries NUM [drop]
```
Anzahl: Der Wert liegt zwischen 1 und 128, mit dem Standardwert 64. Eine gute Zahl für einen schnellen Roaming-Trigger ist in der Regel 32. In den meisten Funkumgebungen ist die Verwendung einer geringeren Anzahl nicht empfehlenswert.

Drop: Wenn dies nicht der Fall ist, startet der WGB ein Roaming-Ereignis, wenn die maximale Anzahl an erneuten Versuchen erreicht wird. Wenn vorhanden, startet der WGB kein neues Roaming und verwendet andere Trigger, wie z. B. Beacon Loss und Signal.

RSSI-Überwachung

WGB kann einen proaktiven Signalscan für das aktuelle übergeordnete Element implementieren und einen neuen Roaming-Prozess starten, wenn das Signal unter den erwarteten Wert fällt.

Dieser Vorgang umfasst zwei Parameter:

- Ein Timer, der den Prüfprozess alle X Sekunden aufruft
- RSSI-Ebene, die verwendet wird, um einen Roaming-Prozess zu starten, wenn das aktuelle Signal darunter liegt.

Beispiel:

```
in d0
mobile station period 4 threshold 75
```
Die Zeit sollte nicht geringer sein als die, die der WGB benötigt, um einen Authentifizierungsprozess abzuschließen, um unter bestimmten Bedingungen eine "Roaming Loop" zu verhindern oder ein zu aggressives Roaming-Verhalten zu vermeiden. Im Allgemeinen sollte getestet werden, um festzustellen, was den Anwendungsanforderungen entspricht.

PSK kann niedriger sein als bei EAP-basierten Methoden (typisch 2 und 4 für sehr aggressive Anwendungen).

Der RSSI-Level wird als positive Ganzzahl ausgedrückt, obwohl es sich im Grunde um einen normalen -dBm-Messwert handelt. Sie sollten eine deutlich höhere Zahl als das Minimum verwenden, das erforderlich ist, um die Datenrate korrekt zu nutzen. Wenn die gewünschte Mindestgeschwindigkeit beispielsweise 6 Mbit/s beträgt, sollte ein Grenzwert von -87 RSSI ausreichen. Für 48 Mbit/s sind -70 dBm usw. erforderlich.

Hinweis: Dieser Befehl kann auch ein "Roaming durch Datenratenänderung" auslösen, das zu aggresiv ist. Es muss zusammen mit einer Mindestrate verwendet werden, um gute Ergebnisse zu erzielen.

Mindestdatenrate

Ab 12.4(25d)JA hat Cisco einen konfigurierbaren Parameter hinzugefügt, um zu steuern, wann der WGB ein neues Roaming-Ereignis auslösen soll, wenn die aktuelle Datenrate für übergeordnete Geräte unter einem bestimmten Wert liegt.

Dies ist hilfreich, um sicherzustellen, dass die gewünschte niedrigere Geschwindigkeit beibehalten wird, um Video- oder Sprachanwendungen zu unterstützen.

Bevor dieser Befehl verfügbar war, löste das WGB häufig ein Roaming aus, wenn die Rate niedriger war als die vorherige. Im Prinzip auf Zeit X+1, wenn die Rate niedriger war als die vorherige X-Zeit, startete die WGB einen Roaming-Prozess. In den Protokollen werden folgende Meldungen angezeigt:

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

Dies ist zu aggregiert, und normalerweise war die einzige Lösung die Konfiguration einer einzelnen Datenrate sowohl im WGB als auch auf übergeordneten APs.

Es wird empfohlen, diesen Befehl immer dann zu konfigurieren, wenn ein mobiler Station-Punkt-Befehl verwendet wird:

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

Dadurch wird der neue Roaming-Prozess nur ausgelöst, wenn die aktuelle Rate niedriger ist als der konfigurierte Wert. Dadurch werden unnötige Roamings reduziert und ein erwarteter Wert für die Rate beibehalten.

Hinweis: Die Meldung `"Had to lower data rate"` wird auch bei dieser Konfiguration erwartet, dass sie jetzt nur noch angezeigt werden sollte, wenn WGB TX mit einer niedrigeren Geschwindigkeit als die konfigurierte Geschwindigkeit war, wenn die Prüfzeit für die Mobilfunkzeit ausgelöst wurde.

Scan-Kanäle

Der WGB scannt alle "Länderkanäle", während er ein Roaming-Ereignis durchführt. Das bedeutet, dass Sie je nach Funkdomäne die Kanäle 1 bis 11 im 2,4-GHz-Band oder 1 bis 13 scannen können.

Jeder gescannte Kanal benötigt einige Zeit. Bei 802.11bg beträgt dieser Wert etwa 10 bis 13 ms. Bei 802.11a kann es bis zu 150 ms betragen, wenn der Kanal DFS-aktiviert ist (also nicht testen, sondern nur passiv scannen).

Eine gute Optimierung besteht darin, die gescannten Kanäle so einzuschränken, dass sie nur die Kanäle verwenden, die von der Infrastruktur in Betrieb genommen werden. Dies ist besonders bei 802.11a wichtig, da die Kanalliste groß ist und die Zeit pro Kanal bei Verwendung von DFS lang sein kann.

Beim Entwurf eines Channel-Plans für WGB/Roaming sind drei Punkte zu beachten:

- Bei einem 2,4-GHz-Frequenzband sollten Sie versuchen, die 1/6/11-Frequenz zu verwenden, um Störungen am Nebenkanal zu minimieren. Jeder andere Kanalplan mit 4 usw. lässt sich aus RF-Sicht meist nur schwer ordnungsgemäß konstruieren, ohne dass die Interferenz zunimmt.
- Die Verwendung einer einzigen Kanaleinrichtung für alle APs ist aus Sicht des Scanners eine gute Idee. Dies ist nur sinnvoll, wenn die Gesamtzahl der zu unterstützenden Clients sehr gering ist und keine hohen Bandbreitenanforderungen bestehen. Dadurch wird die Zeitdauer der Funkumstellung von der Abtastzeit entfernt. Beachten Sie, dass nur wenige Umgebungen von dieser Option profitieren können. Seien Sie daher vorsichtig.
- Für das 5,0-GHz-Band, sofern dies durch Ihre lokalen Richtlinien möglich ist, ermöglicht die

Verwendung von Nicht-DFS-Kanälen (36 bis 48) für den Innenbereich eine schnellere Abtastzeit, da WGB die einzelnen Kanäle aktiv prüfen kann, anstatt länger passives Abhören zu betreiben.

Der für Ihre Bereitstellung verwendete Channel-Plan muss möglicherweise anderen Anforderungen entsprechen. Verwenden Sie die allgemeinen Empfehlungen für das RF-Design.

So konfigurieren Sie die Scan-Kanalliste:

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

Hinweis: Mobilstation wird nur angezeigt, wenn die WGB-Rolle im Radio verwendet wird.

Hinweis: Stellen Sie sicher, dass Ihre WGB-Scan-Liste mit Ihrer Infrastruktur-Channel-Liste übereinstimmt. Andernfalls findet der WGB Ihre verfügbaren APs nicht.

Timer konfigurieren

Ab 12.4(25a)JA gibt es mehrere neue Befehle zur Optimierung des Wiederherstellungs-Timers, wenn ein Problem gefunden wird, die nur verfügbar sind, wenn sich der Access Point im WGB-Modus befindet.

```
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
```

Bei assoc-response, auth-response und client-add gibt diese an, wie lange der WGB auf die Antwort des übergeordneten Access Points warten wird, bevor der Access Point als tot angesehen wird und der nächste Kandidat versucht wird. Die Standardwerte sind 5 Sekunden, was bei einigen Anwendungen zu lang ist. Der Timer ist mindestens 800 ms und wird für die meisten mobilen Anwendungen empfohlen.

Bei eap-timeout legt der WGB eine maximale Wartezeit fest, bis der vollständige EAP-Authentifizierungsprozess abgeschlossen ist. Dies funktioniert aus EAP-Sicht, um den Prozess neu zu starten, wenn der EAP-Authentifizierer nicht zurückantwortet. Der Standardwert ist 60 Sekunden. Achten Sie darauf, niemals einen Wert zu konfigurieren, der geringer sein kann als der tatsächliche Zeitaufwand für den Abschluss einer vollständigen 802.1x-Authentifizierung. Normalerweise ist die Einstellung auf 2 bis 4 Sekunden für die meisten Bereitstellungen richtig.

Für die iApp-Aktualisierung generiert das WGB standardmäßig ein IAPP-Bulk-Update für den übergeordneten Access Point nach dem Roaming, um die bekannten kabelgebundenen Clients zu informieren. Etwa 10 Sekunden später erfolgt eine zweite erneute Übertragung nach der Zuordnung. Dieser Timer ermöglicht die "schnelle Wiederholung" des IAPP-Bulk nach der Zuordnung, um die Möglichkeit zu vermeiden, dass das erste IAPP-Update aufgrund von RF verloren ging, oder Verschlüsselungsschlüssel, die noch nicht auf dem übergeordneten Access Point installiert waren. Bei schnellem Roaming können 100 ms verwendet werden. Stellen Sie jedoch sicher, dass eine große Anzahl von WGB verwendet wird. Dadurch erhöht sich die Gesamtzahl der IAPP, die nach jedem Roaming an die Infrastruktur gesendet werden, erheblich.

Beispiel für aggresive Werte:

```
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
```

Diese wurden in Bereitstellungsszenarien für mobile WGB erfolgreich getestet.

Weitere WGB-Optimierungen

Bei WGB-Bereitstellungsszenarien sind weitere geringfügige Änderungen zu berücksichtigen:

Funkverbindung

- Reduzieren Sie **die Wiederholungsversuche** - **rts versucht 32 erneut**. Dies kann bei Szenarien, in denen die Funkfrequenz gleichzeitig anfällt, einige Zeit einsparen. Normalerweise ist dies nicht erforderlich.
- Antennentyp: Wenn Sie eine einzelne Antenne verwenden (keine Vielfalt), sollten Sie die Funkmodule so konfigurieren, dass die allgemeine Leistung verbessert wird:

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

Antennenvielfalt ist wünschenswert, aber nicht immer möglich, wenn Antennen physisch am Fahrzeug installiert werden. Die richtige Antennenauswahl ist für Roaming entscheidend. Nur 2 dB können einen großen Unterschied im allgemeinen Roaming-Durchschnitt darstellen.

Protokollbezogen

- Um einige Millisekunden zu sparen, reduzieren Sie die Konsolenprotokollierungsebene auf Fehler: **Protokollieren von Konsolenfehlern**. Deaktivieren Sie ihn nicht vollständig, da er unter bestimmten Bedingungen die Roaming-Leistung beeinträchtigen kann.
- Verwenden Sie im Idealfall telnet oder ssh von der Ethernet-Seite, um Debug- oder Protokolldateien zu sammeln. Dies hat im Vergleich zur Protokollierung von Debugging über die Konsole wesentlich geringere Auswirkungen auf die Leistung: **Protokollierung des Überwachungs-Debuggens**.
- Der Befehl, um zu verstehen, was für den WGB-Roaming-Standpunkt geschieht, ist **debug dot11 dot1 0 trace print Uplink**. Dies hat nur geringe Auswirkungen auf die CPU, aktiviert jedoch keine anderen Debugoptionen, es sei denn, es wird angewiesen, dass jede Option die Gesamt-Roaming-Zeit erhöhen kann.
- Versuchen Sie, wenn möglich SNTP zu verwenden. Dadurch bleibt die WGB-Zeit synchron, was bei der Fehlerbehebung sehr hilfreich ist.

MFP-Nutzung

- MFP kann aus sicherheitstechnischer Sicht nützlich sein. Ein Nachteil besteht jedoch darin, dass der WGB bei Roaming-Fehlern keine De-auth-Frames vom übergeordneten Access

Point akzeptiert, um ein neues Roaming auszulösen, wenn der Verschlüsselungsschlüssel zwischen beiden Paketen aus irgendeinem Grund falsch funktioniert.

- In diesen seltenen Fehlerszenarien kann der WGB bis zu 5 Sekunden dauern, bis ein neuer Scan ausgelöst wird, wenn das aktuelle übergeordnete Element mit einem guten Funksignal hörbar ist. Es gibt einen "catch-all"-Erkennungsmechanismus, den WGB auslösen kann, wenn während dieser Zeit keine gültigen Daten-Frames empfangen werden.
- Standardmäßig versucht die WGB, den Client-MFP zu verwenden, wenn die SSID WPA2 AES verwendet.
- Es wird empfohlen, Client-MFP zu deaktivieren, wenn schnelle Wiederherstellungszeiten erforderlich sind (WGB, um auf ungeschützte Standard-Frames zu reagieren). Dies ist ein Kompromiss zwischen Sicherheitsanforderungen und schnellen Wiederherstellungszeiten. Die Entscheidung hängt davon ab, was für das Bereitstellungsszenario wichtiger ist.

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

EAP-TLS auf WGB und "clock save interval"

Weitere Informationen finden Sie im Abschnitt Synchronize IOS Supplicant Clocks and Save Time Setting to NVRAM Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 12.4(21a)JY.

Beachten Sie, dass der uWGB bei Verwendung von uWGB nie die Möglichkeit erhält, eine SNMP-Synchronisierung durchzuführen, da er in der Regel mit der angeschlossenen MAC-Adresse verknüpft ist und die uWGB BVI keinen Netzwerkzugriff hat. Daher wird bei einem uWGB empfohlen, bei der Bereitstellung mindestens eine gute Uhrensynchronisierung im NVRAM zu erzielen. Wenn das angeschlossene Netzwerkgerät als NTP-Quelle fungieren kann (sowie als aktualisierter Client über seine uWGB-Verbindung), kann davon ausgegangen werden, dass die uWGB-SNMP-Synchronisierung als effektiver NTP-Reflektionspunkt dient.

Vollständiges Konfigurationsbeispiel

```
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
```

Debuganalyse

Bei allen auftretenden Problemen ist es wichtig, die Ausgabe des Befehls **debug dot11 dot1 0 trace print Uplink** als ersten Schritt zu erfassen. Dies bietet eine gute Übersicht über den Ablauf

des Roaming-Prozesses.

Dies ist ein Beispiel für ein aktuell übergeordnetes Element als Kandidat:

```
 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
```

Dies ist der Auslöser für das Erreichen eines niedrigen Signals. Dies hängt vom Befehl "mobile station period X threshold Y" ab. Die erste Nachricht wird immer an die Konsole gesendet, die zweite ist Teil der Uplink-Debug-Traces. Dies ist kein Problem, sondern Teil des normalen WGB-Prozesses.

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

Der Uplink-Prozess erzwingt eine Säuberung der Funkwarteschlange, bevor ein Kanalscan gestartet wird. Dieser Schritt kann je nach Kanalnutzung und Warteschlangentiefe einige Millisekunden bis mehrere Sekunden dauern. Daten-Frames werden nicht zum Zeitlimit zurückgesetzt. Bei Sprach-Frames erfolgt ein Zeitvergleich, daher sollte der Vorgang schneller abgebrochen werden. In lauten Umgebungen kann es zu Verzögerungen kommen.

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

Dies ist der eigentliche Kanalscan, der stattfindet. Es parkt das Funkmodul etwa 10 bis 13 ms pro konfiguriertem Kanal.

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

Dies ist die Liste der eingegangenen Sonde-Antworten. Die erste Zahl ist der Kanal, die zweite Mikrosekunden, die für den Empfang benötigt werden.

```
 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
```

Tatsächlicher Vergleich in diesen Details:

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

Übergeordnete Auswahl

```
 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.
```

Dies ist der Punkt, an dem das Roaming abgeschlossen ist. Der Datenverkehr wird fortgesetzt, sobald IAPP-Frames vom übergeordneten Frames verarbeitet werden.

Übergeordnete Vergleichsinformationen

```
 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
```

Wenn der "aktuelle" AP immer noch dem WGB zugeordnet ist, wird der tatsächliche Zuordnungszähler -1 gedruckt (d. h. der WGB selbst wird nicht in der Zahl erfasst), dann werden Hops und Last ausgegeben.

Der Comparison2 druckt die Unterschiede. Deshalb ist es möglich, eine negative Zahl zu sehen. Wenn der Test eine höhere Zahl als die aktuelle aufweist, sehen Sie einen negativen Wert.

Je nach aktueller Zuordnungsanzahl, Last, Signaldifferenz, mobilem Grenzwert kann der WGB ein neues übergeordnetes Element auswählen oder auch nicht.

Der Vergleich findet immer zwischen zwei APs statt, wobei der ausgewählte AP den aktuellen Wert für die nächste Iteration ersetzt. Daher können einige Entscheidungen auf RSSI in einer Schleife oder auf andere Faktoren beim nächsten Test zurückzuführen sein.

Zugehörige Informationen

- Verwendung eines IOS-WGB mit EAP-TLS-Authentifizierung in einem Cisco Unified Wireless Network
- Technischer Support und Dokumentation - Cisco Systems