Häufig gestellte Fragen zu Lightweight Access Points

Inhalt

Einführung

Dieses Dokument enthält Informationen zu den am häufigsten gestellten Fragen (FAQs) zu Cisco Lightweight Access Points (LAPs).

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

Häufig gestellte Fragen zu LAP

F. Was ist ein Cisco Lightweight Access Point (LAP)?

Antwort: Die Cisco LAP ist Teil der Cisco Unified Wireless Network-Architektur. Eine LAP ist ein AP, der an einen WLAN-Controller (WLC) angeschlossen werden soll. Die LAP bietet Dualband-Unterstützung für IEEE 802.11a, 802.11b und 802.11g sowie simultane Funküberwachung für dynamisches Echtzeit-Funkfrequenzmanagement. Darüber hinaus verarbeiten Cisco LAPs zeitkritische Funktionen wie die Layer-2-Verschlüsselung, die Cisco WLANs die sichere Unterstützung von Sprach-, Video- und Datenanwendungen ermöglichen.

APs sind "Lightweight", d. h. sie können nicht unabhängig von einem WLAN Controller (WLC) agieren. Der WLC verwaltet die AP-Konfigurationen und die Firmware. Die APs werden "Zero Touch" bereitgestellt, und eine individuelle Konfiguration der APs ist nicht erforderlich. Die APs sind außerdem leicht, da sie nur Echtzeit-MAC-Funktionen unterstützen. Die APs lassen alle Nicht-Echtzeit-MAC-Funktionen für die Verarbeitung durch den WLC zu. Diese Architektur wird als "Split-MAC"-Architektur bezeichnet.

F. Kann ich die LAP so konfigurieren, dass sie unabhängig von einem WLAN-Controller (WLC) funktioniert?

Antwort: Nein, LAPs können nicht unabhängig von WLCs funktionieren. LAPs funktionieren nur in Verbindung mit einem WLC. Der Grund hierfür ist, dass der WLC alle Konfigurationsparameter und die Firmware bereitstellt, die die LAP für den Registrierungsprozess benötigt.

F. Was ist LWAPP (Lightweight AP Protocol)?

Antwort: LWAPP ist ein IETF-Entwurfsprotokoll (Internet Engineering Task Force), das das Steuerungs-Messaging für die Einrichtung, die Pfadauthentifizierung und Laufzeitoperationen definiert. LWAPP definiert außerdem den Tunneling-Mechanismus für Datenverkehr.

Eine LAP erkennt einen Controller mithilfe von LWAPP-Erkennungsmechanismen. Die LAP sendet eine LWAPP-Join-Anfrage an den Controller. Der Controller sendet der LAP eine LWAPP-Join-Antwort, wodurch der Access Point dem Controller beitreten kann. Wenn die LAP dem Controller beitritt, lädt die LAP die Controller-Software herunter, wenn die Revisionen auf der LAP und dem Controller nicht übereinstimmen. Anschließend wird die LAP vollständig vom Controller kontrolliert. LWAPP sichert die Steuerungskommunikation zwischen der LAP und dem Controller über eine sichere Schlüsselverteilung. Für die sichere Schlüsselverteilung sind sowohl auf der LAP als auch auf dem Controller bereits bereitgestellte digitale X.509-Zertifikate erforderlich. Auf werkseitig installierte Zertifikate wird der Begriff "MIC" verwiesen, ein Akronym für das Zertifikat, das in der Fertigung installiert wurde. Cisco Aironet APs, die vor dem 18. Juli 2005 ausgeliefert wurden, verfügen über kein MIC. Diese APs erstellen also ein selbstsigniertes Zertifikat (SSC), wenn sie aktualisiert werden, um im Lightweight-Modus zu funktionieren. Controller sind so programmiert, dass sie SSCs für die Authentifizierung bestimmter APs akzeptieren.

F. Was ist CAPWAP?

Antwort: In Controller-Software ab Version 5.2 verwenden Cisco Lightweight Access Points das IETF-Standardprotokoll "Control and Provisioning of Wireless Access Points" (CAPWAP), um zwischen dem Controller und anderen Lightweight Access Points im Netzwerk zu kommunizieren. Controller-Softwareversionen vor 5.2 verwenden für diese Kommunikation das LWAPP (Lightweight Access Point Protocol).

CAPWAP basiert auf LWAPP und ist ein standardisiertes, interoperables Protokoll, mit dem ein Controller eine Reihe von Wireless Access Points verwalten kann. CAPWAP wird in der Controller-Software Version 5.2 aus folgenden Gründen implementiert:

- Bereitstellung eines Upgrade-Pfads für Cisco Produkte, die LWAPP verwenden, auf Cisco Produkte der nächsten Generation, die CAPWAP verwenden
- Verwaltung von RFID-Lesegeräten und ähnlichen Geräten
- Damit Controller in Zukunft mit Access Points von Drittanbietern zusammenarbeiten können

LWAPP-fähige Access Points können einen CAPWAP-Controller erkennen und ihm hinzufügen. Die Konvertierung zu einem CAPWAP-Controller erfolgt nahtlos. Beispielsweise sind der Controller-Erkennungsvorgang und der Firmware-Download-Prozess bei Verwendung von CAPWAP identisch mit dem bei Verwendung von LWAPP. Eine Ausnahme bilden Layer-2-Bereitstellungen, die nicht von CAPWAP unterstützt werden.

Sie können CAPWAP-Controller und LWAPP-Controller im selben Netzwerk bereitstellen. Mit der CAPWAP-fähigen Software können Access Points einem Controller beitreten, der CAPWAP oder LWAPP ausführt. Die einzige Ausnahme ist der Cisco Aironet Access Point der Serie 1140, der nur CAPWAP unterstützt und daher nur Controller hinzufügt, die CAPWAP ausführen. Beispielsweise kann ein Access Point der Serie 1130 einem Controller beitreten, der entweder CAPWAP oder LWAPP ausführt, während ein Access Point der Serie 1140 nur einem Controller beitreten kann, der CAPWAP ausführt.

Weitere Informationen finden Sie im Abschnitt Access Point Communication Protocols im Konfigurationsleitfaden.

F. Wie unterscheide ich zwischen einem regulären (autonomen) Access Point und einer LAP?

Antwort: Die einfachste Methode, zwischen einem regulären Access Point und einer LAP zu unterscheiden, ist die Teilenummer des Access Points.

- LAP (Lightweight AP Protocol [LWAPP]): Teilenummern beginnen *immer* mit **AIR-LAPXXXX**.
- Autonomous AP (Cisco IOS® Software) - Teilenummern beginnen *immer* mit **AIR-APXXXX**.

Die Cisco Aironet LAPs der Serie 1000 stellen eine Ausnahme von diesen Kriterien dar. Die Teilenummern der LAPs der Serie 1000 lauten wie folgt:

- AIR-AP1010-A-K9 für 1010 LAP
- AIR-AP1020-A-K9 für 1020 LAP
- AIR-AP1030-A-K9 für 1030 LAP

Hinweis: Die Teilenummern können variieren, je nach Land und Zulassung. Die in dieser Liste enthaltenen Teilenummern sind nur Beispiele.

Stellen Sie sicher, dass Sie den entsprechenden WAP für Ihr WLAN bestellen.

F. Auf welchen AP-Modellen kann LWAPP (Lightweight AP Protocol) ausgeführt werden?

Antwort: Diese Cisco Aironet AP-Plattformen können LWAPP ausführen:

- Aironet Serie 1500
- Cisco Aironet Serie 1250
- Aironet Serie 1240 AG
- Aironet Serie 1230 AG
- Aironet Serie 1200
- Aironet Serie 1130 AG
- Aironet Serie 1000
- Aironet AP der Serie 1140**Hinweis:** Der Access Point der Serie 1140 wird nur von WLC unterstützt, der Version 5.2 oder höher ausführt.

Hinweis: Sie können diese Aironet Access Points mit Cisco IOS Software bestellen, um sie als autonome Access Points zu verwenden oder mit LWAPP zu arbeiten. Die Teilenummer bestimmt, ob es sich bei einem AP um einen Cisco IOS Software-basierten AP oder einen LWAPP-basierten AP handelt. Hier einige Beispiele:

- AIR-AP1242AG-A-K9 ist ein softwarebasierter Cisco IOS-Access Point.
- AIR-LAP1242AG-P-K9 ist ein AP auf LWAPP-Basis.

Hinweis: Von diesem Kriterium ausgenommen sind die APs der Serie 1000 und die APs der Serie 1500. Alle APs der Serie 1000 und die APs der Serie 1500 unterstützen nur LWAPP.

F. Wie installiere und konfiguriere ich einen LWAPP-fähigen Access Point?

Antwort: LWAPP-fähige APs sind Teil der Cisco Integrated Wireless Network Solution und müssen vor der Installation nicht manuell konfiguriert werden. Der Access Point wird von einem LWAPP-fähigen Cisco Wireless LAN Controller (WLC) konfiguriert. Informationen zur Installation und Erstkonfiguration eines LWAPP-fähigen Access Points finden Sie in der Schnellstartanleitung für

LWAPP-fähige Cisco Aironet Access Points.

F. Wie konfiguriere ich meine LAP und meinen Wireless LAN Controller (WLC) zusammen?

Antwort: LAPs verwenden Lightweight AP Protocol (LWAPP). Wenn sie einem WLC beitreten, sendet der WLC den LAPs alle Konfigurationsparameter und die Firmware. Eine grundlegende Einrichtung finden Sie im Konfigurationsbeispiel für den Wireless LAN-Controller und den Lightweight Access Point.

F. Kann ich einen unabhängigen Access Point mit einem WLAN-Controller (WLC) verbinden und erwarten, dass der Access Point funktioniert?

Antwort: Nein, nur LAPs funktionieren, wenn sie mit einem WLC verbunden sind. Autonome APs verstehen weder das Lightweight AP Protocol (LWAPP) noch das CAPWAP-Protokoll, das der WLC verwendet. Um einen autonomen Access Point mit einem WLC zu verbinden, müssen Sie zuerst den autonomen Access Point in den Lightweight-Modus konvertieren.

F. Ich habe einen autonomen Access Point, der auf der Cisco IOS Software basiert. Kann ich es in den Lightweight-Modus umwandeln?

Antwort: Ja, aber nicht alle autonomen AP-Modelle, die auf der Cisco IOS Software basieren, können konvertiert werden. Diese Modelle können in den LWAPP-Modus (Lightweight AP Protocol) konvertiert werden:

- Alle APs der Cisco Aironet 1130 AG
- Alle Aironet APs der Serie 1240 AG
- Für alle modularen APs der Cisco IOS Software-basierten Aironet Serie 1200 (Cisco IOS Software Upgrade, 1210 und 1230 AP)-Plattformen (120/1220, 1210 und 1230 AP) ist die Konvertierung des Access Points vom Funkmodul abhängig.Wenn es sich um IEEE 802.11g-Funkmodule handelt, werden MP21G und MP31G unterstützt.Wenn es sich um IEEE 802.11a-Funkmodule handelt, werden RM21A und RM22A unterstützt.Sie können die APs der Serie 1200 mit einer beliebigen Kombination von unterstützten Funkmodulen aktualisieren:Nur GNur AG und A

Hinweis: Ein autonomer Access Point muss die Cisco IOS Software Version 12.3(7)JA oder höher ausführen, bevor Sie sie in LWAPP umwandeln können.

Hinweis: Nur die Cisco Wireless LAN Controller (WLCs) der Serien 4400 und 2006 unterstützen autonome Access Points, die in den Lightweight-Modus konvertiert wurden. Cisco WLCs müssen eine Softwareversion von mindestens 3.1 ausführen. Das Cisco Wireless Control System (WCS) muss eine Mindestversion von 3.1 aufweisen. Das Aktualisierungsprogramm wird auf den Plattformen Microsoft Windows 2000 und Windows XP unterstützt.

Weitere Informationen zur Durchführung der Konvertierung finden Sie unter Upgrade Autonomous Cisco Aironet Access Points auf Lightweight Mode.

F. Welche Einschränkungen gelten für einen Cisco IOS Software-basierten Access Point nach der Umstellung auf den Lightweight-Modus?

Antwort: Beachten Sie diese Richtlinien, wenn Sie autonome Access Points verwenden, die in den Lightweight-Modus konvertiert wurden:

- APs, die in LWAPP (Lightweight AP Protocol) konvertiert werden, unterstützen keine Wireless Domain Services (WDS). APs, die in LWAPP umgewandelt wurden, kommunizieren nur mit Cisco Wireless LAN (WLAN)-Controllern (WLCs) und können nicht mit WDS-Geräten kommunizieren. Der WLC stellt jedoch Funktionen bereit, die dem WDS entsprechen, wenn der AP dem WLC zugeordnet wird.
- Konvergente Access Points unterstützen nur Controller 2006, 4400 und WiSM. Wenn Sie einen autonomen Access Point in den Lightweight-Modus konvertieren, kann der Access Point mit Cisco Controllern der Serie 2006, Controllern der Serie 4400 oder den Controllern nur auf einem Cisco WiSM kommunizieren.
- In der Controller-Software Version 4.2 oder höher unterstützen alle Cisco Lightweight Access Points 16 BSSIDs pro Funkmodul und insgesamt 16 Wireless LANs pro Access Point. In früheren Versionen wurden nur 8 BSSIDs pro Funkmodul und insgesamt 8 Wireless LANs pro Access Point unterstützt. Wenn ein konvertierter Access Point einem Controller zugeordnet wird, werden nur Wireless-LANs mit den IDs 1 bis 16 an den Access Point weitergeleitet.
- APs, die in LWAPP konvertiert werden, müssen eine IP-Adresse erhalten und den WLC mithilfe von DHCP, einem Domain Name System (DNS) oder einem IP-Subnetz-Broadcast ermitteln.
- APs, die in LWAPP konvertiert werden, unterstützen kein Layer-2-LWAPP.
- APs, die in LWAPP konvertiert werden, stellen einen schreibgeschützten Konsolenport bereit.
- Das Konvertierungstool für Upgrades fügt den selbstsignierten Schlüssel-Hash (SSC) nur einem der Controller im Cisco WiSM hinzu. Nachdem die Konvertierung abgeschlossen ist, fügen Sie den SSC-Schlüssel-Hash dem zweiten Controller im Cisco WiSM hinzu, indem Sie den SSC-Schlüssel-Hash vom ersten Controller auf den zweiten Controller kopieren. Um den SSC-Schlüssel-Hash zu kopieren, öffnen Sie die Seite "AP Policies" (AP-Richtlinien) der Controller-GUI (**Security > AAA > AP Policies**), und kopieren Sie den SSC-Schlüssel-Hash aus der Spalte "SHA1 Key Hash" (Schlüssel-Hash für SHA1) unter "AP Authorization List" (AP-Autorisierungsliste). Öffnen Sie dann mit der GUI des zweiten Controllers die gleiche Seite, und fügen Sie den Schlüssel-Hash unter "AP zur Autorisierungsliste hinzufügen" in das Feld SHA1-Schlüssel-Hash ein. Wenn Sie über mehr als ein Cisco WiSM verfügen, verwenden Sie WCS, um den SSC-Schlüssel-Hash an alle anderen Controller zu übertragen.

Weitere Informationen finden Sie in den Versionshinweisen für Cisco Aironet Access Points der Serien 1130AG, 1200, 1230AG und 1240AG für Cisco IOS Release 12.3(7)JX.

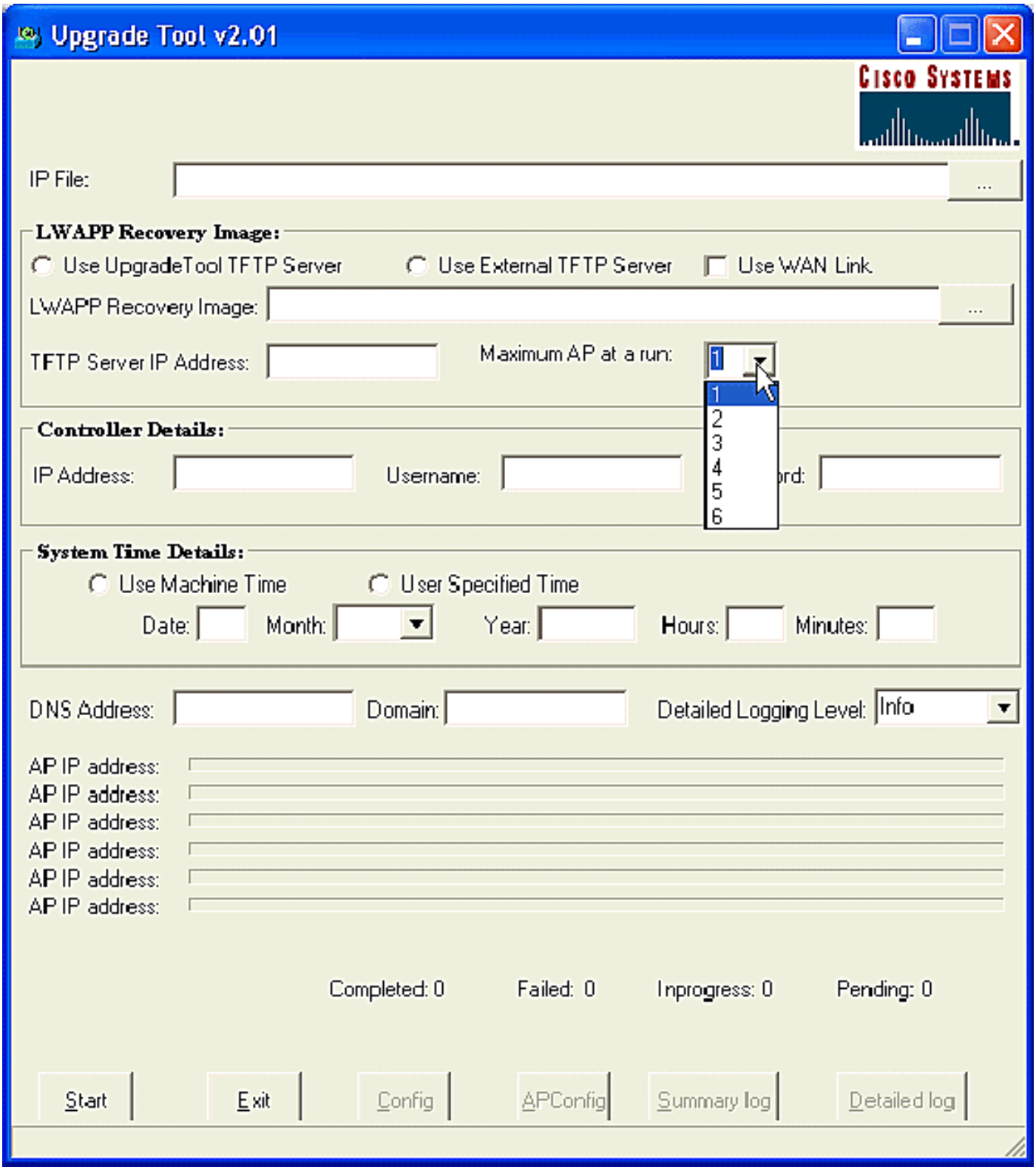
F. Ich habe meinen Access Point in den Lightweight-Modus konvertiert, aber ich muss ihn wieder in den autonomen Modus umwandeln. Ist das möglich?

Antwort: Ja, Sie können autonome APs, die Sie in den Lightweight-Modus konvertiert haben, in den autonomen Modus zurücksetzen. Führen Sie die Schritte im Abschnitt *Konvertieren eines Lightweight Access Points zurück in den Autonomous Mode (Autonomous Mode)* des Upgrades autonomer Cisco Aironet Access Points in den Lightweight Mode aus.

F. Wie viele Access Points können gleichzeitig über das Upgrade-Tool konvertiert werden?

Antwort: Mit der neuesten Version 2.01 des Tools können Sie maximal sechs APs gleichzeitig

aktualisieren.



F. Ich habe meinen AP in Lightweight AP Protocol (LWAPP) konvertiert, aber der Access Point registriert sich nicht beim Controller. Ich erhalte die Meldung "`LWAPP Join-Request enthält kein gültiges Zertifikat in CERTIFICATE_PAYLOAD vom AP`". Was verursacht dieses Problem?

Antwort: Dieser Fehler bedeutet, dass die digitalen X.509-Zertifikate ungültig sind. Möglicherweise haben Sie die Cisco Bug ID CSCsd42296 (nur registrierte Kunden). Die Lösung für dieses Problem besteht darin, die Access Points auf die Werkseinstellungen zurückzusetzen.

Eine weitere Möglichkeit besteht darin, dass das selbstsignierte Zertifikat (SSC) nicht beim WLC registriert ist. Eine manuelle Hinzufügung des SSC am Controller kann erforderlich sein. Weitere Informationen zum Verfahren finden Sie unter Manuelles Hinzufügen von selbstsignierten Zertifikaten zum Controller für LWAPP-konvertierte APs.

F. Kann ich einen Cisco IOS Software-basierten Access Point als Arbeitsgruppen-Bridge konfigurieren und mit LWAPP-basierten APs (Lightweight AP Protocol) verknüpfen?

Antwort: Sie können einen Access Point so konfigurieren, dass er als Workgroup Bridge betrieben wird, sodass er Wireless-Verbindungen zu einem Lightweight Access Point für Clients bereitstellen kann, die über Ethernet mit dem Workgroup Bridge Access Point verbunden sind. Wenn Sie den Access Point so konfigurieren, dass er als Arbeitsgruppen-Bridge fungiert und eine Verbindung zu einem Cisco Unified Network herstellt, kann er kabelgebundene Clients, die über Ethernet mit dem Arbeitsgruppen Bridge Access Point verbunden sind, Wireless-Verbindungen bereitstellen. Wenn Sie beispielsweise Wireless-Verbindungen für eine Gruppe von kabelgebundenen Geräten bereitstellen müssen, können Sie die Geräte mit einem Hub oder Switch verbinden, den Hub oder Switch mit dem Ethernet-Port des Access Points verbinden und den Access Point als Arbeitsgruppen-Bridge konfigurieren.

Das Dokument Workgroup Bridges in a Cisco Unified Wireless Network Configuration Example enthält ein Konfigurationsbeispiel.

F. Kann ein Wireless-Client zwischen LWAPP-APs und autonomen APs wechseln?

Antwort: Nein, Roaming zwischen LAPs und autonomen APs wird NICHT unterstützt. Der Grund hierfür ist, dass der Datenverkehr bei der Verbindung mit LWAPP-APs über einen LWAPP-Tunnel geleitet wird. Da zwischen dem Wireless LAN Controller und den autonomen APs kein Mobility Tunnel vorhanden ist, funktioniert das Roaming nicht.

F. Welche Antennenoptionen stehen für die verschiedenen Modelle der Cisco Aironet LAPs der Serie 1000 zur Verfügung?

Antwort: Das LAP-Gehäuse der Serie 1000 enthält:

- Eine IEEE 802.11a- oder eine 802.11b/g-Funkantenne
- Vier interne Hochverstärkungsantennen (zwei 802.11a und zwei 802.11b/g)

Sie können diese Antennen unabhängig voneinander aktivieren oder deaktivieren, um eine 180-Grad-Rundstrahlabdeckung oder einen 360-Grad-Rundstrahlbereich zu erzeugen. Einige der LAPs der Serie 1000 können auch externe Antennen verwenden. Die LAPs der Serie 1000 sind in drei Modellen erhältlich:

- LAP 1010
- LAP 1020
- LAP 1030

Folgende Antennenoptionen stehen zur Verfügung:

- LAP 1010:Vier interne Antennen mit hoher VerstärkungKeine externen Antennenadapter vorhanden
- LAP 1020:Vier interne Antennen mit hoher VerstärkungEin externer 5-GHz-

AntennenadapterZwei externe 2,4-GHz-Antennenadapter

- 1030 LAP (Remote-Edge LAP):Vier interne Antennen mit hoher VerstärkungEin externer 5-GHz-AntennenadapterZwei externe 2,4-GHz-Antennenadapter

A. External-Antenna Model B. Internal-Antenna Model

Hinweis: Die LAPs der Serie 1000 müssen die werksseitig bereitgestellten internen oder externen Antennen verwenden, um eine Verletzung der FCC-Anforderungen zu vermeiden und zu verhindern, dass die Benutzerautorisierung zum Betrieb der Geräte außer Kraft tritt.

F. Welche Stromversorgungsoptionen stehen für die Cisco Aironet LAPs der Serie 1000 zur Verfügung?

Antwort: Die Aironet LAP der Serie 1000 kann von einem externen 110- bis 220-V-AC-zu-48-V-Gleichstrom-Netzteil oder von Power over Ethernet-Geräten mit Strom versorgt werden. Das externe Netzteil (AIR-PWR-1000) wird an eine sichere 110 bis 220 V AC-Steckdose angeschlossen. Der Konverter erzeugt die erforderliche 48-V-Gleichstromausgabe für die LAP der Serie 1000. Die Konverterausgabe wird über eine 48-V-Gleichstrombuchse an die Seite der LAP der Serie 1000 eingezogen.

Hinweis: Sie können das externe Netzteil AIR-PWR-1000 mit länderspezifischen Netzkabeln bestellen. Wenden Sie sich bei Ihrer Bestellung an Cisco, um das richtige Netzkabel zu erhalten.

F. Kann ich Telnet/SSH in einen LWAPP-basierten Access Point integrieren?

Antwort: In Wireless LAN Controller Version 5.0 und höher unterstützt der Controller die Verwendung von Telnet- oder Secure Shell (SSH)-Protokollen zur Fehlerbehebung bei Lightweight Access Points. Sie können diese Protokolle verwenden, um das Debuggen zu

vereinfachen, insbesondere wenn der Access Point keine Verbindung zum Controller herstellen kann. Sie können die Telnet- und SSH-Unterstützung nur über die Controller-CLI konfigurieren.

Um die Telnet- oder SSH-Konnektivität auf einem Access Point zu aktivieren, verwenden Sie die **Konfigurationsübersicht {Telnet | ssh}**-Befehl. Der Cisco Lightweight Access Point verbindet sich mit diesem Cisco Wireless LAN Controller für den gesamten Netzwerkbetrieb und bei einem Hardware-Reset.

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

Beispiele

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

F. So konfigurieren Sie globale Anmeldeinformationen für Access Points. Wie lauten der Standardbenutzername und das Standardkennwort in Version 5.0?

Antwort: Cisco IOS Access Points werden werkseitig mit Cisco als Standard-enable-Kennwort ausgeliefert. Mit diesem Kennwort können Benutzer sich im nicht privilegierten Modus anmelden und Befehle zum Anzeigen und Debuggen ausführen, was eine Sicherheitsbedrohung darstellt. Das Standardkennwort für die Aktivierung muss geändert werden, um nicht autorisierten Zugriff zu verhindern und um Benutzern die Ausführung von Konfigurationsbefehlen über den Konsolenport des Access Points zu ermöglichen.

In der Controller-Software vor Version 5.0 können Sie das enable-Kennwort des Access Points nur für Access Points festlegen, die derzeit mit dem Controller verbunden sind. In der Controller-Software Version 5.0 können Sie einen globalen Benutzernamen, ein Kennwort und ein Kennwort festlegen, das alle Access Points erben, sobald sie dem Controller beitreten. Dies umfasst alle Access Points, die derzeit dem Controller angeschlossen sind, sowie alle Access Points, die in Zukunft hinzugefügt werden. Auf Wunsch können Sie die globalen Anmeldeinformationen überschreiben und einen eindeutigen Benutzernamen, ein Kennwort und das Kennwort für einen bestimmten Access Point zuweisen.

Informationen zum Konfigurieren der globalen Anmeldeinformationen des Access Points finden Sie unter Konfigurieren globaler Anmeldeinformationen für Access Points.

F. Ich habe Wireless LAN Controller (WLC) 2006 und Access Point (AP) 1242 mit Firmware-Version 3.2.78.0. Ich habe Probleme mit Access Points, die eine Verbindung herstellen, und erhalte folgende Fehlermeldungen: "lwapp_cliet_error;erhält keine Leseantwort(3). Lwapp_image_broc;TAR-Datei kann nicht geöffnet werden"

Antwort: AP 1242 sind konvertierte LWAPP-APs (Lightweight Access Point Protocol). Wenn Sie konvertieren und versuchen, sie zu verwenden, versuchen sie, nach dem Controller zu suchen, um ihm beizutreten. Wenn die APs den Controller nicht finden, wird dieser Meldungstyp auf der Konsole angezeigt. In diesem Fall verfügt der Controller jedoch über eine Firmware-Version

3.2.78.0, die nicht mit aktualisierten APs kompatibel ist. Sie benötigen die Firmware-Version 3.2.116.21, um mit aktualisierten APs arbeiten zu können. Nach dem Upgrade der Controller-Firmware schließen sich diese APs dem Controller an und beginnen zu funktionieren.

F. Clients zeigen eine MAC-Adresse von 00:17:0f:37:65:c4, wenn sie an einen Access Point angeschlossen sind, aber der Access Point zeigt, dass er eine Radio MAC-Basisadresse von 00:17:0f:37:65:c0 hat. Warum zeigt der Client eine andere MAC-Adresse an als der Access Point? Gibt es eine Möglichkeit zu bestimmen, welche MAC-Adresse das Gerät registriert, wenn ich zwei Access Points mit sehr engen MAC-Adressen habe?

Antwort: Wenn Sie sich einen Access Point im Detailmodus ansehen, können Sie sehen, dass er über eine Radio MAC-Basisadresse und eine FastEthernet MAC-Adresse verfügt. Darüber hinaus ist dies die grundlegende Radio MAC-Adresse, die sich mit dem WLAN ändert. Der Client sieht die BSSID in Form einer MAC-Adresse.

F. Ich habe ein bestehendes Wireless-Netzwerk (autonome APs) mit einem Access Point, der als Repeater konfiguriert ist. Dieses Netzwerk soll zu einem LWAPP-Wireless-Netzwerk migriert werden. Kann ich die LWAPP APs als Repeater verwenden?

Antwort: LWAPP-APs müssen einem Controller angeschlossen sein, und sie unterstützen keinen Repeater-Modus, da alle über eine gewisse Anbindung an den Controller verfügen müssen. Autonomous Access Points von Cisco können als Repeater konfiguriert werden. Aufgrund der geringeren effektiven Bandbreite für Endclients sind Repeater jedoch nicht die am meisten empfohlene Konfiguration. Während jedes Cisco Aironet AP- oder LAP-Modell entweder im LWAPP- oder im autonomen Modus verwendet werden kann, ist für diese Änderung ein Software-Reimage erforderlich. Dies ist besonders komplex, wenn es von autonom zu LWAPP wechselt, sodass direkt, nein, ein AIR-LAP1232AG-A-K9 den Repeater-Modus nicht nativ unterstützt. Es könnte mit autonomer Software geladen werden und so gemacht werden, dass der Repeater-Modus unterstützt wird. Dies würde jedoch eine Softwareänderung und eine separate Konfiguration erfordern.

F. Wie viele APs können von WLCs unterstützt werden?

Antwort: Die Anzahl der pro WLC unterstützten APs hängt von der Modellnummer ab:

- **2106** - Ein eigenständiger WLC, der bis zu 6 APs mit 8 Fast Ethernet-Schnittstellen unterstützt.
- **4402**: Ein eigenständiger WLC, der 12, 25 oder 50 APs unterstützt.
- **4404**: Ein eigenständiger WLC, der 100 APs unterstützt.
- **5500** - Ein eigenständiger WLC, der 12, 25, 50, 100 oder 250 Access Points für geschäftskritische Wireless-Services an Standorten jeder Größe unterstützt.
- **WLCM** - Ein WLC-Modul, das speziell für die Integrated Service Router (ISR)-Serie von Cisco entwickelt wurde. Es ist derzeit als 6-, 8- oder 12-AP-Version erhältlich.
- **WS-C3750G** - Ein WLC, der entweder 25 oder 50 APs unterstützt, die in den Catalyst 3750 Switch integriert sind. Die Backplane-Verbindungen des WLC werden als 2-Gigabit-Ethernet-Ports angezeigt, die separat als dot1q-Trunks konfiguriert werden können, um die Verbindung zum 3750 bereitzustellen. Alternativ können die Gig-Ports als Link aggregiert werden, um eine

einzelne EtherChannel-Verbindung zum 3750 bereitzustellen. Da der WLC direkt integriert ist, hat er Zugriff auf alle erweiterten Routing- und Switching-Funktionen des 3750 Stackable Switches. Dieser WLC eignet sich ideal für mittelgroße Büros oder Gebäude. Die Version "50 AP" kann auf bis zu 200 APs skaliert werden, wenn vier 3750-Access Points als virtueller Switch in einem Stack zusammengefasst werden.
- **WiSM** - Ein WLC-Modul, das speziell für die Cisco Catalyst Switches der Serie 6500 entwickelt wurde. Sie unterstützt bis zu 300 APs pro Modul. Je nach Plattform der Serie 6500 können mehrere WISMs installiert werden, um eine erhebliche Skalierbarkeit zu ermöglichen. Das WiSM wird auf dem 6500 als zentrale Schnittstelle für aggregierte Verbindungen angezeigt, die als Dot1-Trunk konfiguriert werden kann, um die Verbindung zur 6500-Backplane herzustellen. Dieses Modul eignet sich ideal für große Gebäude oder Campus.

F. Wie viele Clientzuordnungen können von Access Points maximal unterstützt werden?

Antwort: Die maximale Anzahl von Clientzuordnungen, die von den Access Points unterstützt werden können, hängt von folgenden Faktoren ab:

- Die maximale Anzahl von Clientzuordnungen unterscheidet sich bei Lightweight- und Autonmous IOS-Access Points.
- Pro Funkmodul kann ein Limit und ein Limit pro AP vorhanden sein.
- AP-Hardware (APs mit 16 MB haben eine niedrigere Obergrenze als APs mit 32 MB und mehr).

Vollständige Einzelheiten zu den Client-Zuordnungsbeschränkungen finden Sie im Abschnitt *Client Association Limits* im Konfigurationshandbuch für Cisco Wireless LAN Controller, Version 7.0.

F. Unterstützt der 1252 AP Bridging?

Antwort: Ja, der Bridging-Modus wird vom Access Point der Serie 1252 unterstützt.

F. Unterstützt die LWAPP-Infrastruktur (Lightweight AP Protocol) PPP over Ethernet (PPPoE) (PC-Client zu einem PPPoE-Server)?

Antwort: Nein, die LWAPP-Infrastruktur unterstützt PPPoE nicht. Der Grund hierfür ist, dass der PPPoE-Ethertype-Modus am Controller verworfen wird.

F. Wie kann ich die Cisco Aironet LAP der Serie 1000 manuell zurücksetzen?

Antwort: Sie können den Access Point über den WLAN-Controller (WLC) auf die Werkseinstellungen zurücksetzen. Für das Zurücksetzen sollte die LAP beim WLC registriert werden.

Führen Sie diese Schritte aus:

1. Klicken Sie in der WLC-GUI auf **Wireless**. Die Registerkarte Wireless bietet Zugriff auf die Konfiguration des Wireless-Netzwerks der Cisco WLAN-Lösung.
2. Wählen Sie **Access Points > Cisco APs aus**, und klicken Sie dann auf **Detail**, um zum

Fenster für den jeweiligen Access Point zu navigieren.

3. Klicken Sie unten in diesem Fenster auf **Konfiguration löschen**. Dadurch wird die Konfiguration auf der LAP gelöscht und auf die Werkseinstellungen zurückgesetzt.

Um die LAPs mithilfe der Kommandozeile auf die Werkseinstellungen zurückzusetzen, führen Sie den Befehl **clear ap-config *ap-name* aus der WLC-CLI aus.**

F. Wo erhalte ich weitere Informationen zu den Cisco Aironet LAPs der Serie 1000?

Antwort: Weitere Informationen erhalten Sie in den Fragen und Antworten zu den Lightweight Access Points der Cisco Serie 1000. Das Dokument enthält Antworten auf viele Fragen zu den LAPs der Serie 1000.

F. Welche Cisco Geräte unterstützen den LWAPP-Layer-2-Modus (Lightweight AP Protocol)?

Antwort: Der LWAPP Layer 2-Modus wird nur auf folgenden Cisco Geräten unterstützt:

- Cisco Wireless LAN Controller (WLC) der Serie 4100
- Cisco WLC der Serie 4400
- Cisco Aironet LAP der Serie 1000

F. Wenn ich richtig verstanden habe, verwenden die Cisco LAPs für die Controller-Erkennung eine VCI-Zeichenfolge (Vendor Class Identifier) mit DHCP-Option 43. Welcher VCI-Zeichenfolgenwert gilt für Cisco LAPs?

Antwort: Die APs der Cisco Aironet 1000-Serie verwenden für die DHCP-Option 43 ein Zeichenfolgenformat, während die anderen Aironet-APs das TLV-Format (Type, Length, Value) für die DHCP-Option 43 verwenden. Sie müssen DHCP-Server programmieren, um die Option auf Basis der DHCP-VCI-Zeichenfolge (DHCP-Option 60) zurückgeben zu können. Diese Tabelle enthält die VCI-Zeichenfolgenwerte für die verschiedenen LAPs:

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

F. Welche Bedeutung haben die TLV-Blockwerte (Type Length Value) in Bezug auf die DHCP-Option 43? Wie wird der TLV-Wert berechnet?

Antwort: Die DHCP-Option 43 kann mit dem folgenden Befehl auf dem DHCP-Server des Cisco IOS-Routers aktiviert werden:

```
Option 43 hex <string>
```

Die Hexadezimalzeichenfolge in diesem Befehl wird durch Verkettung der TLV-Werte für die Unteroption 43 zusammengesetzt.

Typ + Länge + Wert

- **Type** ist immer der Code der Unteroption 0xf1.
- **Length** ist die Anzahl der IP-Adressen für die Controller-Verwaltung mal 4 in Hex.
- **Value** ist die IP-Adresse des Controllers, die sequenziell in Hexadezimalziffern aufgeführt ist.

Beispiel: Es gibt zwei Controller mit den IP-Adressen 10.126.126.2 und 10.127.127.2 der Verwaltungsschnittstelle:

- Der Typ ist 0xf1.
- Die Länge ist 2 x 4 = 8 = 0 x 08.
- Die IP-Adressen werden in 0a7e7e02 (10.126.126.2) und 0a7f7f02 (10.127.127.2) übersetzt.
- Beim Zusammenstellen der Zeichenfolge wird f1080a7e7e020a7f7f02 ausgegeben. Der dem DHCP-Bereich hinzugefügte IOS-Befehl lautet:

  ```
  option 43 hex f1080a7e7e020a7f7f02
  ```

F. Unterstützt der Wireless LAN Controller (WLC) den AP-Lastenausgleich?

Antwort: Ja, Sie können AP-Lastenausgleich auf einem WLC ausführen. Weitere Informationen finden Sie in den Häufig gestellten Fragen zur Fehlerbehebung für Wireless LAN Controller (WLC).

F. Wie konfiguriere ich das WLC-Failover (Wireless LAN Controller) für LAPs?

Antwort: Weitere Informationen zur Konfiguration des WLC-Failovers finden Sie im Konfigurationsbeispiel für WLAN-Controller-Failover für Lightweight Access Points.

F. Wie kann ich die Reset-Taste auf den APs nach der Umwandlung vom autonomen in den Lightweight-Modus deaktivieren?

Antwort: Sie können die Reset-Taste bei APs deaktivieren, die Sie in den Lightweight-Modus konvertiert haben. Die Reset-Taste ist an der Außenseite des Access Points mit "MODE" (MODE) gekennzeichnet. Verwenden Sie diesen Befehl, um die Reset-Taste für einen oder alle konvertierten APs zu deaktivieren oder zu aktivieren, die einem Controller zugeordnet sind:

config ap reset-button {enable | disable} {*ap-name* | all}
Die Reset-Taste für konvertierte APs ist standardmäßig aktiviert.

F. Kann ein LWAPP-fähiger Access Point über eine WAN-Verbindung mit dem WLAN-Controller (WLC) verbunden sein? Wenn ja, wie funktioniert das?

Antwort: Ja, einige LAPs unterstützen die Funktion "Remote-Edge AP (REAP)". Mit dieser Funktion können Sie eine LAP über eine WAN-Verbindung vom WLC, mit dem die LAP verbunden ist, einrichten. Der REAP-Modus ermöglicht es einer LAP, sich über eine WAN-Verbindung aufzuhalten, mit dem WLC zu kommunizieren und die Funktionalität einer regulären LAP bereitzustellen. Ein detailliertes Beispiel für diese Einrichtung finden Sie im Konfigurationsbeispiel für Remote-Edge AP (REAP) mit einfachen APs und Wireless LAN Controllern (WLCs).

Hinweis: Der REAP-Modus wird derzeit nur auf den Cisco Aironet 1030 LAPs unterstützt. Die REAP-Funktion wird zukünftig in eine breitere Palette von LAPs integriert werden.

F. Verfügen wir bei Access Points im Überwachungsmodus immer noch über dieselben WAN-Beschränkungen wie bei regulären APs und H-REAPs? Benötigen wir also eine 100 ms oder besser RTD zwischen dem Controller und einem Überwachungsmodus-AP?

Antwort: Nein, der Access Point im Überwachungsmodus verfügt nicht über die 100-ms-Einschränkung, da keine Client-Zuordnung vorhanden ist. Dies ist der Grund für die Einschränkung. Die Latenzbeschränkung von 100 ms wurde aus unterschiedlichen, oft strengen Client-Autorisierungsanforderungen erstellt. Aus diesem Grund gelten für den lokalen Modus und für H-REAPs identische Latenzbeschränkungen. Natürlich verfügen APs im Überwachungsmodus nicht über die gleichen Client-Beschränkungen.

F. Meine WLC-Version ist 3.2. Sie wird für das Layer 3 Lightweight Access Point Protocol (LWAPP) konfiguriert. Die MTU für das Netzwerk zwischen diesem WLC und meinem Lightweight Access Point (LAP) wird als 900 Byte konfiguriert. Mein LWAPP AP kann diesem WLC nicht beitreten. Was kann der Grund dafür sein?

Antwort: Die im Szenario konfigurierte MTU beträgt 900 Byte. Eine LWAPP Join-Anforderung ist jedoch größer als 1500 Byte. Hier benötigt LWAPP ein Fragment der LWAPP Join-Anforderung. Die Logik für alle LWAPP-APs lautet, dass die Größe des ersten Fragments 1500 Byte beträgt (einschließlich IP- und UDP-Header) und das zweite Fragment 54 Byte (einschließlich IP- und UDP-Header). Wenn das Netzwerk zwischen LWAPP-APs und dem WLC eine MTU-Größe von weniger als 1500 (z. B. VPN, GRE, MPLS usw.) aufweist, kann der WLC die Anforderung der LWAPP-Join-Verbindung nicht bearbeiten. Aus diesem Grund kann das LWAPP dem Controller nicht beitreten.

Aktualisieren Sie Ihren Controller auf Version 4.0, um dieses Problem zu beheben. Diese Version kann Layer-3-Fragmente verarbeiten. Weitere Informationen zu diesem Problem finden Sie unter Cisco Bug ID CSCsd94967 (nur registrierte Kunden).

F. Ich habe einen WLC, den ich aus Singapur bekommen habe. Mit diesem WLC beabsichtigte ich, eine Remote Office-Verbindung (REAP) für Wireless-Verbindungen herzustellen. Ich habe Büros in anderen Ländern. Allerdings erhalte

ich vom Singapore WLC Fehlermeldungen zu regulatorischen Domänen. Besteht die Möglichkeit, den WLC dazu zu zwingen, Access Points (APs) mit unterschiedlichen Zulassungsdomänen zu akzeptieren? Die Fehlermeldung, die ich erhalte, lautet: "**AP 'AP_NAME' kann keine Verbindung herstellen. Die auf diesem '-R' konfigurierte Zulassung stimmt nicht mit dem Ländercode des Controllers 'A.B.C.D' 'SG - Singapur'** überein.

Antwort: Der WLC unterstützt nur eine Zulassung. Aus diesem Grund kann ein WLC, der die regulatorische Domäne -A verwendet, nur mit APs verwendet werden, die die regulatorische Domäne -A verwenden (usw.). In diesem Fall ist der WLC auf -SG für Singapur festgelegt, sodass er nur APs in der aufsichtsrechtlichen Domäne Singapurs unterstützt.

Wenn Sie APs und WLCs erwerben, müssen Sie sicherstellen, dass diese dieselbe regulatorische Domäne verwenden. Erst dann können sich die Access Points beim WLC registrieren.

Unterstützung von mehreren Ländercodes - Mit WLC Version 4.1.171.0 und höher wird die Unterstützung von mehreren Landescodes mit WLCs eingeführt. Ab Version 4.1.171.0 können Sie bis zu 20 Ländercodes pro Controller konfigurieren. Durch die Unterstützung mehrerer Ländercodes können Access Points in verschiedenen Ländern über einen einzigen Controller verwaltet werden. Diese Funktion wird für die Verwendung mit Cisco Aironet Mesh Access Points nicht unterstützt.

F. In welchen Modi kann ein Lightweight Access Point (LAP) betrieben werden?

Antwort: Eine LAP kann in einem der folgenden Modi betrieben werden:

- **Local Mode (Lokaler Modus)**: Dies ist der Standardmodus für den Betrieb. Wenn eine LAP in den lokalen Modus geschaltet wird, wird der Access Point über den normalerweise zugewiesenen Kanal übertragen. Der Access Point überwacht jedoch auch alle anderen Kanäle im Frequenzband über einen Zeitraum von 180 Sekunden, um jeden anderen Kanal während der nicht übertragenen Zeit für 60 ms zu scannen. Während dieser Zeit misst der Access Point den Geräuschpegel, misst Störungen und scannt nach IDS-Ereignissen.
- **REAP-Modus** - Der Remote Edge Access Point (REAP)-Modus ermöglicht es einer LAP, sich über einen WAN-Link aufzuhalten, dennoch mit dem WLC kommunizieren zu können und die Funktionalität einer regulären LAP bereitzustellen. Der REAP-Modus wird nur auf den 1030 LAPs unterstützt.
- **H-REAP Mode** - H-REAP ist eine Wireless-Lösung für Bereitstellungen in Zweigstellen und Zweigstellen. Mit H-REAP können Kunden Access Points (APs) in einer Zweigstelle oder in einer Außenstelle über eine WAN-Verbindung konfigurieren und steuern, ohne dass in jedem Büro ein Controller bereitgestellt werden muss. H-REAPs können den Client-Datenverkehr lokal umschalten und die Client-Authentifizierung lokal ausführen, wenn die Verbindung zum Controller unterbrochen wird. Wenn H-REAPs mit dem Controller verbunden sind, können sie auch den Datenverkehr zurück zum Controller leiten.
- **Überwachungsmodus** - Der Überwachungsmodus ist eine Funktion, die es bestimmten LWAPP-fähigen APs ermöglicht, sich von der Verarbeitung des Datenverkehrs zwischen Clients und der Infrastruktur auszuschließen. Stattdessen fungieren sie als dedizierte Sensoren für standortbasierte Services, Erkennung von nicht autorisierten Access Points und Intrusion Detection (IDS). Wenn sich APs im Überwachungsmodus befinden, können sie keine Clients versorgen und durchlaufen kontinuierlich alle konfigurierten Kanäle, die jedem

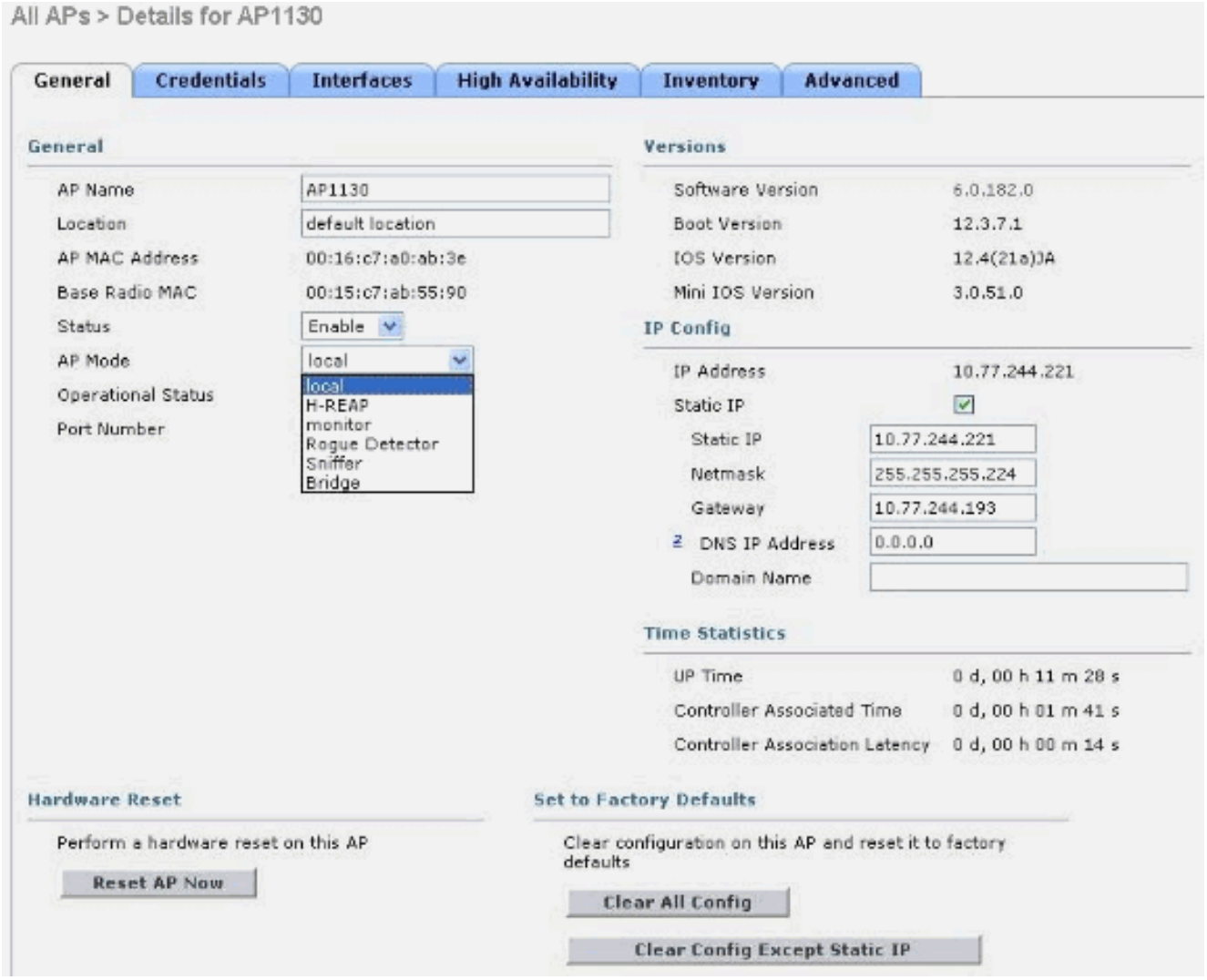
Kanal ungefähr 60 ms lang lauschen.**Hinweis:** Ab Controller Release 5.0 können LWAPPs auch im Location Optimized Monitor Mode (LOMM) konfiguriert werden, der die Überwachung und Standortberechnung von RFID-Tags optimiert. Weitere Informationen zu diesem Modus finden Sie unter Cisco Unified Wireless Network Software Release 5.0.**Hinweis:** Mit Controller Version 5.2 wurde der **LOMM-**Bereich (**Location Optimized Monitor Mode)** in **Tracking Optimization** umbenannt, und das Dropdown-Feld **LOMM Enabled** wurde in **Enable Tracking Optimization umbenannt**.**Hinweis:** Weitere Informationen zum Konfigurieren der Tracking-Optimierung finden Sie im Abschnitt Optimizing RFID Tracking on Access Points (RFID-Optimierung für Access Points optimieren).

- **Rogue-Detektor-Modus**: LAPs, die im Rogue Detector-Modus arbeiten, überwachen die nicht autorisierten Access Points. Sie übertragen keine nicht autorisierten APs oder enthalten diese. Die Idee dahinter ist, dass der nicht autorisierte Detektor alle VLANs im Netzwerk sehen kann, da nicht autorisierte APs mit einem beliebigen VLAN im Netzwerk verbunden werden können (so verbinden wir es mit einem Trunk-Port). Der Switch sendet alle nicht autorisierten AP/Client-MAC-Adresslisten an den Rogue Detector (RD). Der RD leitet diese dann an den WLC weiter, um sie mit den MACs von Clients zu vergleichen, die die WLC APs per Funk gehört haben. Wenn MACs übereinstimmen, weiß der WLC, dass sich der nicht autorisierte Access Point, mit dem diese Clients verbunden sind, im kabelgebundenen Netzwerk befindet.
- **Sniffer-Modus** - Ein LWAPP, der im Sniffer-Modus betrieben wird, fungiert als Sniffer und erfasst und leitet alle Pakete auf einem bestimmten Kanal an einen Remotecomputer, der Airopeek ausführt. Diese Pakete enthalten Informationen zu Zeitstempel, Signalstärke, Paketgröße usw. Die Sniffer-Funktion kann nur aktiviert werden, wenn Sie Airopeek ausführen, eine Netzwerkanalyse-Software eines Drittanbieters, die die Decodierung von Datenpaketen unterstützt.
- **Bridge Mode** - Der Bridge-Modus wird verwendet, wenn die Access Points in einer Mesh-Umgebung eingerichtet und zum Bridging zwischen den Access Points verwendet werden.

F. Wie ändere ich den Modus bei einem Lightweight Access Point?

Antwort: Führen Sie die folgenden Schritte aus, um den Modus eines Lightweight Access Points zu ändern.

1. Wählen Sie in der WLC-GUI **Wireless > Access Points > All APs (Wireless > Access Points > Alle APs) aus**, und wählen Sie den Access Point aus, für den der Modus geändert werden muss, und wählen Sie aus der Liste der registrierten APs aus.
2. Die Seite **All APs > Details for AP** wird angezeigt. Wählen Sie auf der Registerkarte **Allgemein** dieser Seite den **AP-Modus** aus dem Dropdown-Menü aus, wie folgt:



F. Ich habe neu installierte LAP-1131AG Access Points installiert, die für einen bestimmten Controller konfiguriert wurden. Meine Controller-Version ist 4.0.155.5. Wenn ich sie mit demselben Wireless LAN Controller (WLC) starte, für den sie eingerichtet sind, leuchtet diese letztendlich grün. Gemäß der Dokumentation bedeutet dieses hellgrüne Licht an der Status-LED, dass sie mit dem WLC verbunden sind. Dieser Access Point wurde jedoch nicht in der Liste der Access Points des WLC aufgeführt. Warum ist das so? Wurde das LWAPP (Lightweight Access Point Protocol) verknüpft?

Antwort: Wenn der Access Point auf einem WLC auf Layer 3 konfiguriert ist, aber beim Start keine IP-Adresse erhält, leuchtet die Status-LED des WLC grün und geht erst in die Such- und Neustartsequenz über, wenn er eine IP-Adresse von DHCP erhält.

In solchen Szenarien zeigt die Status-LED, die grün leuchtet, nicht an, dass das LWAPP beim Controller registriert ist. Wenn die Access Points ihre DHCP-Adressen erhalten haben, suchen sie nach dem WLC und führen, falls diese nicht gefunden werden, einen Neustart durch, und fahren Sie wie erwartet fort. Hiermit ist ein Fehler verbunden.

Weitere Informationen finden Sie unter Cisco Bug ID CSCsf10580 (nur registrierte Kunden).

F. Was zeigen die LEDs an der LAP an?

Antwort: Dies ist ein Link zu einem kurzen Video, in dem erläutert wird, wie die LEDs eines Lightweight AP der Serie 1130AG interpretiert werden:

Interpretieren von LAP-LEDs - LAP1130

F. Worin besteht der Unterschied zwischen RAPs (Roof-Top Access Points) und PAPs (Pole-Top Access Points) als Modi von MAPs (Lightweight Mesh Access Points)?

Antwort: Dies sind die Modi, die die MAPs für Außenbereiche als Teil des Mesh-Netzwerks verwenden können. Die Mesh-Netzwerklösung, die Teil der Cisco Unified Wireless Network-Lösung ist, ermöglicht es zwei oder mehr Cisco Aironet Lightweight MAPs, über einen oder mehrere Wireless-Hops miteinander zu kommunizieren, um mehreren LANs beizutreten oder die 802.11b-Wireless-Abdeckung zu erweitern.

Diese Access Points werden als Teil des Mesh-Netzwerks verwendet und können in zwei Modi betrieben werden:

1. RAP
2. PAP

RAP - Cisco MAPs, die im RAP-Modus betrieben werden, sind der übergeordnete Knoten für ein Bridging- oder Mesh-Netzwerk und verbinden eine Bridge oder ein Mesh-Netzwerk mit dem kabelgebundenen Netzwerk. Daher kann für jedes Bridge- oder Mesh-Netzwerksegment nur ein RAP vorhanden sein. In einem Mesh-Netzwerk werden Cisco MAPs konfiguriert, überwacht und von und über jeden bereitgestellten Cisco WLAN Controller (WLC) betrieben. Jeder MAP, der über eine kabelgebundene Verbindung zum WLC verfügt, übernimmt die Rolle des RAP. Dieser RAP verwendet die Wireless-Backhaul-Schnittstelle, um mit benachbarten PAPs zu kommunizieren.

PAP - Cisco MAPs, die im PAP-Modus betrieben werden, haben keine kabelgebundene Verbindung zu einem Cisco WLC. Dabei kann es sich um vollständig drahtlose Clients handeln, die mit anderen PAPs oder RAPs kommunizieren, oder sie können zum Herstellen von Verbindungen zu Peripheriegeräten oder einem kabelgebundenen Netzwerk verwendet werden. Der Ethernet-Port ist aus Sicherheitsgründen standardmäßig deaktiviert. Sie sollten ihn jedoch für PAPs aktivieren.

Im Abschnitt Konfiguration ohne Benutzereingriffe des Bereitstellungsleitfadens für die Cisco Mesh Networking-Lösung finden Sie weitere Informationen dazu, wie ein MAP die Rolle von RAP und PAP übernimmt.

F. Wie interpretieren Sie das Strahlungsmuster der Lightweight Access Point (LAP)-Antennen der Serie 1000?

Antwort: Azimuth-Diagramme sind in der Regel mit dem Gerät/der Antenne in normaler Betriebsausrichtung (vertikal, oben, in der Mitte des Diagramms für Omni; horizontal, in der Mitte montieren, im Diagramm nach vorne Richtung "0"). Die A-Seite ist höchstwahrscheinlich vorwärts und repräsentiert bei der 0-Markierung für Azimut und die 90-Zeichen für Höhenlage. Die B-Seite wird bei der 180-Marke für Azimut und 270 für Höhenangaben repräsentiert. Wenn die Einheit invertiert ist, ändert sich das Muster nicht im Freien. Aber die unmittelbaren Oberflächen können Reflexion/Absorption verursachen und das Muster verändern. Metallische Objekte in der Nähe der Heizkörper (etwa innerhalb von ~2 Wellenlängen) können das Muster auch signifikant verzerren. Der Cisco Aironet Antenna-Referenzhandbuch enthält weitere Informationen. Die Antennen der

Serie 1000 werden im letzten Abschnitt des Dokuments erläutert.

F. Können wir einschränken, welche APs einem Controller beitreten? Ich sehe die Seite "SECURITY/AAA/AP Policies" (SICHERHEITS-/AAA-/AP-Richtlinien), auf der Sie APs anhand des AAA- oder Zertifikats autorisieren können. Ich kann einen Access Point zur Autorisierungsliste hinzufügen, aber schränken diese Vorgänge nur meine Autorisierungsliste der APs ein, dem Controller beizutreten?

Antwort: Nein, die Controller verarbeiten APs auf Basis des First-come-First-Server-Verfahrens. Sie können möglicherweise mit den primären, sekundären und tertiären Feldern spielen, um die Chancen auf AP-Verbindungen zu Ihrer Präferenz zu erhöhen.

F. Kann mit LWAPP die SSIDs eines Access Points auf individueller AP-Basis ermittelt werden? Was ist erforderlich, um bestimmte APs in einer Zone haben zu können, die eine eindeutige SSID verwenden, und alle anderen, die andere SSIDs verwenden?

Antwort: Mit der WLAN-Überschreibungsoption können Sie auswählen, welche SSIDs ein WAP anbietet. Controller unterstützen jeweils nur bis zu 16 SSIDs, sodass Sie nur aus den 16 unterstützten auswählen können. Dies erfolgt auf AP-Basis.

F. Wenn ich einige LWAPP-Befehle auf meiner LAP aktiviere, wird eine Fehlermeldung ausgegeben, dass der Befehl deaktiviert ist. Warum ist das so?

```
AccessPoint#clear lwapp ap controller ip address
ERROR!!! Command is disabled.
```

Antwort: Sobald Ihr AP einem Controller erfolgreich beigetreten ist, werden die LWAPP-Befehle deaktiviert. Um die LWAPP-Befehle erneut zu aktivieren, müssen Sie den Benutzernamen/das Kennwort des Access Points über die Controller-CLI mit dem Befehl **config ap username <name> password <pwd> <cisco-ap>/all** festlegen. Danach können Sie eine **klare lwapp private-config** in der AP-CLI vornehmen, um die Konfigurationsbefehle des AP-LWAPP manuell erneut auszugeben.

Hinweis: Wenn Sie WLC Version 5.0 oder höher ausführen, verwenden Sie diesen Befehl, um den Benutzernamen und das Kennwort für den Access Point festzulegen:

```
config ap mgmtuser add username AP_username password AP_password secret secret {all | Cisco_AP}
```

F. Wenn sich zwei APs auf demselben Kanal befinden und sich gegenseitig sehen können, welche Auswirkungen hat dies (für den Roaming-Durchsatz usw.) auf die Verwendung von vier statt drei Kanälen? Wie reagieren die APs in einer solchen Situation und wie reagiert ein Kunde?

Antwort: Unabhängig davon, ob sich APs auf demselben Kanal befinden oder nicht, wirkt sich dies nicht besonders auf das Client-Roaming aus. Dabei kommt es auf eine ausreichende Zellüberschneidung an, sodass Clients reibungslose Übergänge vom Abdeckungsbereich eines

Access Points zum nächsten durchführen können. Der Übergang von einem Design mit drei Kanälen zu einem Design mit vier Kanälen zielt darauf ab, die Design-Flexibilität zu erhöhen (aufgrund des "zusätzlichen" Kanals). Dieser Ansatz ist kurzsichtig, da Sie zwar eine gewisse Bereitstellungsflexibilität hinzufügen (da Sie einen anderen Kanal haben), aber die Anzahl der Co-Channel-Interferenzen tatsächlich erhöhen. Die Designflexibilität bei einem Vier-Kanal-Ansatz lässt bei zusätzlichen Kanalinterferenzen keine erwarten. Fazit: Verwenden Sie kein Vier-Kanal-Design.

F. Können wir kontrollieren, wann Clients roamen? Können wir den Client nur aufgrund der Signalstärke auf individueller AP-Basis und für alle Client-Adapter roamen lassen?

Antwort: Heute ist Roaming immer eine Funktion des Clients, und die Wahl, Roaming zu nutzen oder nicht, wird in verschiedenen Clients unterschiedlich umgesetzt. Directed Roaming ist Teil von CCX, ist jedoch eine optionale Funktion und wird derzeit nicht verwendet.

F. Gibt es spezifische Anforderungen oder Empfehlungen für eine WAN-Verbindung, die zwischen dem REAP/HREAP am Remote-Standort und dem WLC am Hauptstandort implementiert wird?

Antwort: Dies sind einige der wichtigsten Faktoren, die für die WAN-Verbindung berücksichtigt werden sollten:

- Stellen Sie sicher, dass die Bandbreite der WAN-Verbindung mindestens 128 Kbit/s beträgt.
- Stellen Sie sicher, dass die Latenz oder Round-Trip-Verzögerung zwischen den beiden Standorten über die WAN-Verbindung nicht mehr als 300 ms beträgt, da eine Verzögerung von mehr als 300 ms zu Authentifizierungsproblemen für den Client führen kann, insbesondere wenn eine zentrale Authentifizierung implementiert ist.

F. Ich hatte ein Netzwerk für einige Stunden heruntergefahren, aufgrund dessen die LAPs die Kommunikation mit WLCs verloren. Nach der Netzwerkwiederherstellung haben die LAPs die IP-Adresse vom DHCP-Server übernommen, obwohl diese APs mit einer statischen IP-Adresse konfiguriert sind. Im Feld "`show ap config general <ap-name>`" wird die `IP-Adresse für Fallback` angezeigt. Warum geschieht das?

Antwort: Die LAP versucht, bis zu 20 Mal mit LWAPP-Erkennungsnachrichten eine Verbindung zum WLC herzustellen. Falls keine Verbindung hergestellt werden kann, versucht sie, über DHCP eine neue IP-Adresse zu erhalten. Wenn die LAP eine IP-Adresse vom DHCP-Server beziehen kann, ist diese IP-Adresse die aktive Adresse, und die statisch zugewiesene IP-Adresse wird als Fallback verwendet. Die Idee dahinter ist, dass LAPs, die in ein anderes VLAN (z. B. in ein anderes Gebäude) verschoben werden, eine IP-Adresse abrufen und einem WLC beitreten können. Dieses Verhalten wird im Fehler CSCse66714 erläutert. Sie müssen das WLC auf die Software Version 4.0.206.0 aktualisieren.

F. Muss ein Bridge-Gruppenname für ein Mesh-Netzwerk konfiguriert werden?

Antwort: Ein Bridge-Gruppen-Name (BGN) kann verwendet werden, um die Access Points im Mesh logisch zu gruppieren. Obwohl die APs standardmäßig einen NULL-Wert BGN enthalten, um die Zuordnung zu ermöglichen, empfehlen wir, einen BGN festzulegen. Sie können diese

Konfigurationsänderung über die CLI oder GUI mit dem folgenden Befehl vornehmen:

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

Hinweis: BGNs können maximal zehn Zeichen enthalten. Wenn Sie mehr als 10 Zeichen in das BGN-Feld auf der Konfigurationsseite des GUI-Mesh-Access Points des Controllers eingeben, wird eine Fehlermeldung generiert. Ein Fehler wird auch angezeigt, wenn Sie diesen Parameter über den **Befehl config ap bridgegroupname set groupname Cisco_MAP** CLI oder WCS (CSCsk64812) konfigurieren.

Wenn Sie BGN in einem Live-Netzwerk konfigurieren, stellen Sie sicher, dass Sie die Konfiguration vom am weitesten entfernten MAP aus vornehmen und den Weg zurück zum RAP finden. Dies ist sehr wichtig, da Sie eine untergeordnete MAP anfügen können, die nicht mit einem übergeordneten MAP verknüpft werden kann, der über einen aktualisierten BGN verfügen kann. Verwenden Sie verschiedene BGNs, um verschiedene Teile Ihres Netzwerks logisch zu gruppieren. Dies ist in Situationen nützlich, in denen RAPs im gleichen RF-Bereich vorhanden sind und Segmente Ihres Netzes getrennt bleiben sollen.

Wenn Sie einem Live-Netzwerk einen neuen Access Point hinzufügen möchten, müssen Sie den BGN auf dem neuen Access Point vorkonfigurieren. Wenn Sie das Mesh-Netzwerk von Grund auf mit neuen, sofort einsatzbereiten APs aufrufen, wird in den APs der BGN auf NULL festgelegt. APs werden mit diesem Standardwert des BGN einem neuen Netzwerk hinzugefügt. Mit dem folgenden Befehl können Sie den BGN eines Access Points überprüfen:

```
show ap config general Cisco AP
```

F. Was geschieht, wenn der BGN nicht richtig konfiguriert ist?

Antwort: Wenn der Access Point in Abhängigkeit vom Netzwerkdesign fälschlicherweise mit einem anderen Bridgegroupnamen als dem, für den er bestimmt ist, bereitgestellt wird, kann oder kann dieser Access Point den richtigen Sektor oder Baum ermitteln. Wenn sie einen kompatiblen Sektor nicht erreichen kann, kann sie festgefahren werden. Um einen solchen stranded Access Point wiederherzustellen, wurde das Konzept des standardmäßigen Bridgegroupname eingeführt. Die Grundidee besteht darin, dass ein Access Point, der mit seinem konfigurierten Bridgegroupnamen keine Verbindung zu einem anderen Access Point herstellen kann, versucht, eine Verbindung mit dem Bridgegroupnamen des Standards herzustellen.

Dieser Algorithmus wird zum Erkennen dieser Stranbedingung und zur Wiederherstellung verwendet:

1. Scannen Sie passiv alle benachbarten Knoten, unabhängig von ihrem Bridgegroupnamen.
2. Der Access Point versucht, eine Verbindung zu den Nachbarn herzustellen, die mit einem eigenen Bridgegroupnamen über das Adaptive Wireless Path Protocol (AWPP) erkannt werden.
3. Wenn Schritt 2 fehlschlägt, versuchen Sie, eine Verbindung mit dem standardmäßigen Bridgegroupnamen über AWPP herzustellen.
4. Führen Sie bei jedem fehlgeschlagenen Versuch von Schritt 3 aus der Liste der Nachbarn aus, und versuchen Sie, eine Verbindung zum nächsten besten Nachbarn herzustellen.
5. Wenn der Access Point in Schritt 4 keine Verbindung mit allen Nachbarn herstellen kann, starten Sie den Access Point neu.
6. Wenn die Verbindung mit dem standardmäßigen Bridgegroupnamen 30 Minuten lang

hergestellt ist, scannen Sie alle Kanäle erneut, und versuchen Sie, eine Verbindung mit dem richtigen Bridgegroupnamen herzustellen.

Hinweis: Wenn ein Access Point mit dem standardmäßigen Bridgegroupnamen verbunden werden kann, meldet der übergeordnete Knoten den Access Point als standardmäßigen untergeordneten/Knoten/Nachbareintrag im WLAN-Controller, sodass ein Netzwerkadministrator den gestrandeten Access Point erkennt. Ein solcher Access Point kann weder Client- noch andere Mesh-Knoten als untergeordnete Knoten akzeptieren noch Datenverkehr weiterleiten.

F. Kann eine LAP 1030-Bridge mit anderen Bridge-Modellen verbunden werden? Kann eine LAP 1020 auch Bridging unterstützen?

Antwort: Das Modell LAP 1020 unterstützt kein Bridging. Die LAP 1030 unterstützt Bridging (ein Hop) zu einer anderen LAP 1030, derzeit jedoch nicht zu einem BR1310, BR1400 oder LAP 1500.

F. Kann Wireless Bridging zwischen LAP-APs eingerichtet werden? Ich möchte, dass ein Funkmodul meiner nicht-kabelgebundenen LAPs das Bridging zurück zu den LAN-Root-Bridge-LAPs (LAP verbunden mit einem WLC) durchführt. Ist das möglich?

Antwort: Nein. Dies ist bei LAP-APs nicht möglich. Mesh-APs können ein einfaches Punkt-zu-Punkt-Bridging in einem Cisco Unified Wireless Network durchführen. Die einzige weitere mögliche Bridging-Option ist über IOS APs im WGB-Modus (Workgroup Bridge) möglich. Diese IOS APs fungieren als Clients (mit kabelgebundenen Geräten dahinter) für einen LAP-AP. Wireless-Clients können jedoch keine Verbindung zu diesen IOS-APs herstellen.

F. Ich habe eine LAP 1131, und dieser Access Point ist erfolgreich bei den Wireless LAN Controllern registriert. Wenn ich den Access Point ohne Power Injector anschließe, sind die Funkmodule aktiv (LED-Status grün), aber wenn ich den Access Point mit dem Power Injector verbinde, sind die Funkmodule ausgefallen (LED-Status ist orange). Wie kann ich dieses Problem beheben?

Antwort: Dieses Problem kann auf falsch konfigurierte Power over Ethernet (POE)-Parameter zurückzuführen sein. Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Klicken Sie auf **Wireless**, um auf diese Parameter zuzugreifen.
2. Klicken Sie auf den Link **Detail** des gewünschten Access Points. Die neuen Parameter werden auf der Seite Alle APs > Details unter den POE-Einstellungen angezeigt.
3. Klicken Sie auf der Seite APs > Details des Access Points für die POE-Einstellungen auf **Power Injector State** (Status des Power Injectors), und wählen Sie **Installed (Installiert)** aus.
4. Aktivieren Sie das Kontrollkästchen, um den Status des Power Injectors für den Access Point zu aktivieren. Dieser Parameter ist erforderlich, wenn der angeschlossene Switch IPM nicht unterstützt und ein Power Injector verwendet wird. Dieser Parameter ist nicht erforderlich, wenn der angeschlossene Switch IPM unterstützt.

F. In autonomen APs wird mithilfe von Public Secure Packet Forwarding (PSPF) verhindert, dass Client-Geräte, die diesem AP zugeordnet sind, Dateien versehentlich mit anderen Client-Geräten im Wireless-Netzwerk gemeinsam nutzen. Gibt es eine entsprechende Funktion in Lightweight APs?

Antwort: Die Funktion oder der Modus, der die ähnliche Funktion von PSPF in einer Lightweight-Architektur ausführt, wird als Peer-to-Peer-Blockierungsmodus bezeichnet. Der Peer-to-Peer-Blockierungsmodus ist für die Controller verfügbar, die die LAP verwalten.

Wenn dieser Modus auf dem Controller deaktiviert ist (dies ist die Standardeinstellung), können die Wireless-Clients über den Controller miteinander kommunizieren. Wenn der Modus aktiviert ist, wird die Kommunikation zwischen Clients über den Controller blockiert.

Es funktioniert nur bei APs, die demselben Controller angeschlossen sind. Wenn dieser Modus aktiviert ist, werden Wireless-Clients, die auf einem Controller terminiert sind, nicht daran gehindert, Wireless-Clients über einen anderen Controller zu erreichen, selbst wenn sie sich in derselben Mobilitätsgruppe befinden.

F. Kann ein LAP-AP SNMP-Nachrichten wie einen IOS-AP verarbeiten?

Antwort: Die LAP-APs können SNMP-Meldungen nicht eigenständig verarbeiten. Um SNMP-Meldungen zu verarbeiten, sollten Sie eine SNMP-Community auf dem WLC konfigurieren, auf dem die LAP registriert ist. Alle AP-Informationen werden vom WLC verwaltet.

Zugehörige Informationen

- Häufig gestellte Fragen zur Fehlerbehebung für Wireless LAN Controller (WLC)
- Cisco Wireless LAN Controller-Module
- Häufig gestellte Fragen zum Cisco Wireless LAN Controller (WLC)
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 3.2
- Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point
- Technischer Support und Dokumentation für Cisco Systeme