Implementierungsleitfaden für Indoor Mesh

Inhalt

Einführung
Übersicht
Unterstützte Hardware und Software
Innenbereich und Außenbereich
Konfiguration
Controller-L3-Modus
Aktualisieren des Controllers auf den neuesten Code
MAC-Adresse
Aufzeichnen der MAC-Adresse in den Radios
Geben Sie die MAC-Adresse und die Namen der Funkmodule im Controller ein.
MAC-Filterung aktivieren
L3 Indoor Mesh-Bereitstellung
Definieren von Schnittstellen im Controller
Funkrollen
Bridge-Gruppen-Name
Sicherheitskonfiguration
Installation
Voraussetzungen
Installation
Konfiguration von Stromversorgung und Kanal
RF-Prüfung
Überprüfen der Verbindungen
Zugriffssicherheit der AP-Konsole
Ethernet-Bridging
Erweiterung des Bridge-Gruppen-Namens
Protokolle - Nachrichten, Sys, AP und Trap
Nachrichtenprotokolle
AP-Protokolle
Trap-Protokolle
Leistung
Startup Convergence-Test
WCS
Indoor Mesh-Alarme
Mesh-Bericht und Statistiken
Verbindungstest
Node-to-Node-Verbindungstest
On-Demand-AP-Nachbarverbindungen

Ping-Test
Fazit
Zugehörige Informationen

Einführung

Der Lightweight Access Point 1242/1131 ist ein Wi-Fi-Infrastrukturgerät mit zwei Funkmodulen für ausgewählte Bereitstellungen in Innenbereichen. Es handelt sich um ein LWAPP-basiertes Produkt (Lightweight Access Point Protocol). Er verfügt über ein 2,4-GHz-Funkmodul und ein 5,8-GHz-Funkmodul, das mit 802.11b/g und 802.11a kompatibel ist. Eine Funkeinheit kann für den lokalen (Client-)Zugriff für den Access Point (AP) verwendet werden, die zweite Funkeinheit kann für das Wireless-Backhaul konfiguriert werden. LAP1242/LAP1131 unterstützt P2P-, P2MP- und Mesh-Architekturen.

Lesen Sie sich das Handbuch durch, bevor Sie versuchen, eine der Installationen durchzuführen.

Dieses Dokument beschreibt die Bereitstellung von Enterprise Wireless Mesh für Indoor Mesh. Dieses Dokument ermöglicht es Wireless-Endbenutzern, die Grundlagen von Indoor Mesh zu verstehen, wo ein Indoor Mesh konfiguriert werden muss und wie ein Indoor Mesh konfiguriert wird. Ein Mesh für Innenräume ist eine Teilmenge von Cisco Enterprise Wireless Mesh, die mithilfe von Wireless-Controllern und einfachen APs bereitgestellt wird.

Das Indoor-Mesh ist ein Teil der Enterprise Mesh-Architektur, die auf der Unified Wireless-Architektur bereitgestellt wird. Indoor Mesh ist heute gefragt. Bei Innenvermaschung wird eines der Funkmodule (i. d. R. 802.11b/g) und/oder die kabelgebundene Ethernet-Verbindung für die Verbindung mit Clients verwendet, während das zweite Funkmodul (i. d. R. 802.11a) für das Backhauling des Client-Datenverkehrs verwendet wird. Beim Backhaul kann es sich um einen einzelnen Hop oder über mehrere Hops handeln. Ein Innenmaschinenvermaschung bringt Ihnen diese Werte:

- Ethernet-Kabel müssen nicht für jeden AP ausgeführt werden.
- Ethernet-Switch-Port ist nicht für jeden AP erforderlich.
- Netzwerkverbindungen, bei denen Kabel keine Konnektivität bieten können.
- Flexibilität bei der Bereitstellung - nicht auf 100 m von einem Ethernet-Switch entfernt.
- Einfache Bereitstellung eines Ad-hoc-Wireless-Netzwerks

Große Einzelhändler sind aufgrund der Kosteneinsparungen bei der Verkabelung und der zuvor genannten Gründe sehr attraktiv für Indoor-Mesh.

Lagerspezialisten verwenden sie für die Durchführung von Inventarzählungen für Einzelhändler, Fertigungsbetriebe und andere Unternehmen. Sie möchten an einem Kundenstandort schnell ein temporäres Wi-Fi-Netzwerk bereitstellen, um Echtzeit-Verbindungen für ihre Handheld-Geräte zu ermöglichen. Zu den Orten, an denen Mesh-Architektur für Innenräume erforderlich ist, gehören Bildungsseminare, Konferenzen, Fertigung und Gastfreundschaft.

Wenn Sie diesen Leitfaden vollständig gelesen haben, erfahren Sie, wo Sie das Mesh für Innenräume verwenden und wie Sie es konfigurieren. Sie werden auch verstehen, dass Innenvermaschung in NEMA-Gehäusen KEINEN Ersatz für Outdoor Mesh darstellt. Darüber hinaus werden Sie auch die Überlegenheit der von autonomen APs verwendeten einheitlichen Hops-Mesh-over-Link-Rollenflexibilität (Single-Hop Mesh) verstehen.

Annahmen:

Sie verfügen über umfassende Kenntnisse zu Cisco Unified Wireless Network, der Architektur und den Produkten. Sie kennen die Outdoor Mesh-Produkte von Cisco und einige der für Mesh-Netzwerke verwendeten Terminologie.

Glossar der Akronyme	
LWAPP	Lightweight Access Point Protocol - Das Kontroll- und Datentunnelprotokoll zwischen APs und dem Wireless LAN Controller.
WLAN-Controller/Controller/WLC	Wireless LAN Controller - Cisco Geräte, die die Netzwerkverwaltung eines WLAN zentralisieren und vereinfachen, indem sie eine große Anzahl verwalteter Endgeräte in einem einzigen, einheitlichen System zusammenfassen und so ein einheitliches WLAN-Netzwerksystem mit intelligenten Informationen ermöglichen.
RAP	Root Access Point/Roof Access Point - Cisco Wireless-Geräte fungieren als Bridge zwischen dem Controller und anderen Wireless APs. APs, die mit dem Controller verkabelt sind.
MAP	Mesh-APs - Cisco Wireless-Gerät, das über eine 802.11a-Funkeinheit mit einem RAP oder einem MAP verbunden ist und darüber hinaus Clients über eine 802.11b/g-Funkeinheit anbietet.
Übergeordnet	Ein Access Point (entweder ein RAP/MAP), der über eine 802.11a-Funkeinheit den Zugriff auf andere APs über die Luft ermöglicht.
Nachbarin	Alle APs in einem Mesh-Netzwerk sind Nachbarn und haben Nachbarn. RAP verfügt nicht über einen Nachbarn, da er mit dem Controller verkabelt ist.

Kind	Ein AP, der weiter vom Controller entfernt ist, ist immer ein untergeordnetes Element. Ein Kind hat ein übergeordnetes Element und viele Nachbarn in einem vermaschten Netzwerk. Wenn die übergeordnete Instanz stirbt, wird der nächste Nachbar mit dem besten Leichtigkeit als übergeordneter Wert ausgewählt.
SNR	Signal-Rausch-Verhältnis
BGN	Bridge-Gruppen-Name
EAP	Erweiterbares Authentifizierungsprotokoll
PSK	Vorinstallierter Schlüssel
AWPP	Adaptives Wireless Path Protocol

Übersicht

Der Cisco Indoor Mesh Network Access Point ist ein Wi-Fi-Infrastrukturgerät mit zwei Funkmodulen für ausgewählte Bereitstellungen in Innenräumen. Es handelt sich um ein LWAPP-basiertes Produkt (Lightweight Access Point Protocol). Er verfügt über ein 2,4-GHz-Funkmodul und ein 5,8-GHz-Funkmodul, das mit den Standards 802.11b/g und 802.11a kompatibel ist. Ein Funkmodul (802.11b/g) kann für den lokalen (Client-)Zugriff auf den Access Point verwendet werden, und die zweite Funkeinheit (802.11a) kann für das Wireless-Backhaul konfiguriert werden. Es bietet eine Indoor-Mesh-Architektur, in der verschiedene Knoten (Funkmodule) über Backhaul miteinander kommunizieren und auch lokalen Client-Zugriff bereitstellen. Dieser AP kann auch für Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Bridging-Architekturen verwendet werden. Die Wireless Indoor Mesh Network-Lösung eignet sich ideal für eine große Abdeckung in Gebäuden, da Sie hohe Datenraten und eine gute Zuverlässigkeit bei minimaler Infrastruktur aufweisen können. Dies sind die wichtigsten Funktionen, die mit der ersten Version dieses Produkts eingeführt wurden:

- Wird in Indoor-Umgebungen für eine 3-Hop-Anzahl verwendet. Maximal 4.
- Relay-Knoten und Host für Endbenutzer-Clients. Eine 802.11a-Funkeinheit wird als Backhaul-Schnittstelle und eine 802.11b/g-Funkeinheit für die Wartung von Clients verwendet.
- Sicherheit von Indoor Mesh APs - EAP und PSK werden unterstützt.
- Die LWAPP-MAPs in einer Mesh-Umgebung kommunizieren mit den Controllern auf die gleiche Weise wie die Ethernet-angeschlossenen APs.
- Point-to-Point Wireless Bridging
- Punkt-zu-Mehrpunkt-Wireless-Bridging
- Optimale übergeordnete Auswahl. SNR, EASE und BGN
- BGN-Erweiterungen. NULL- und Standardmodus.
- Lokaler Zugriff.

- Übergeordnete schwarze Liste. Ausschlussliste.
- Selbstheilung mit AWPP
- Ethernet-Bridging
- Grundlegende Unterstützung von Voice ab Version 4.0.
- Dynamische Frequenzauswahl.
- Anti-stranding - Standard-BGN und DHCP-Failover.

Hinweis: Diese Funktionen werden nicht unterstützt:

- 4,9-GHz-Kanal für öffentliche Sicherheit
- Routing um Interferenzen
- Hintergrundprüfung
- Universeller Zugriff
- Unterstützung von Arbeitsgruppen-Bridges

Indoor Mesh-Software

Indoor Mesh Software ist eine spezielle Version, da sie sich auf die Access Points in Innenräumen konzentriert, insbesondere Indoor Mesh. In dieser Version arbeiten sowohl die Access Points für Innenräume im lokalen Modus als auch im Bridge-Modus. Einige der in Version 4.1.171.0 verfügbaren Funktionen sind in dieser Version nicht implementiert. Verbesserungen wurden an der Kommandozeilenschnittstelle (CLI), der grafischen Benutzeroberfläche (GUI - Webbrowser) und am Statuscomputer selbst vorgenommen. Ziel dieser Verbesserungen ist es, aus Ihrer Sicht wertvolle Informationen über dieses neue Produkt und seine Funktionsfähigkeit zu erhalten.

Spezielle Verbesserungen für Innenmaschennetze:

- **Innenumgebung** - Das Innenmaschenetz wird mithilfe von LAP1242s und LAP1131 implementiert. Diese werden in Innenbereichen implementiert, in denen kein Ethernet-Kabel verfügbar ist. Die Implementierung ist einfach und schneller, um eine Wireless-Abdeckung für entfernte Bereiche im Gebäude bereitzustellen (z. B. Einzelhandelsvertriebszentren, Bildungswesen für Seminare/Konferenzen, Fertigung, Gastgewerbe).
- **BGN-Erweiterungen (Bridge Group Name):** Damit Netzwerkadministratoren ein Netzwerk von Indoor Mesh Access Points in benutzerdefinierte Sektoren organisieren können, bietet Cisco einen Mechanismus namens Bridge Group Name (BGN). Der BGN, in der Tat der Sektorname, veranlasst einen Access Point, eine Verbindung zu anderen APs mit demselben BGN herzustellen. Wenn ein Access Point keinen geeigneten Sektor findet, der mit seinem BGN übereinstimmt, wird der Access Point im Standardmodus betrieben, und es wird der beste übergeordnete Port ausgewählt, der auf den Standard-BGN reagiert. Diese Funktion wurde bereits vor Ort sehr geschätzt, da sie gegen die Bedingungen des stranded APs kämpft (wenn jemand das BGN falsch konfiguriert hat). In der Softwareversion 4.1.171.0 funktionieren die APs bei Verwendung des Standard-BGNs nicht als Mesh-Knoten für Innenbereiche und haben keinen Client-Zugriff. Der Zugriff erfolgt im Wartungsmodus über den Controller. Wenn der Administrator das BGN nicht repariert, wird der Access Point nach 30 Minuten neu gestartet.
- **Sicherheitsverbesserungen** - Die Sicherheit im Indoor-Mesh-Code wird standardmäßig für EAP (Extensible Authentication Protocol) konfiguriert. Dies ist in RFC 3748 definiert. Obwohl das EAP-Protokoll nicht auf WLANs beschränkt ist und für die Authentifizierung von LANs verwendet werden kann, wird es in der Regel in WLANs verwendet. Wenn EAP von einem 802.1X-fähigen NAS-Gerät (Network Access Server) wie einem 802.11 a/b/g Wireless Access Point aufgerufen wird, können moderne EAP-Methoden einen sicheren

Authentifizierungsmechanismus bereitstellen und einen sicheren PMK (paarweise Master Key) zwischen Client und NAS aushandeln. Der PMK kann dann für die Wireless-Verschlüsselungssitzung verwendet werden, die TKIP- oder CCMP-Verschlüsselung (basierend auf AES) verwendet.Vor der Softwareversion 4.1.171.0 wurden über Outdoor Mesh Access Points PMK/BMK zum Controller hinzugefügt. Dies war ein Prozess mit drei Zyklen. Jetzt werden die Zyklen für eine schnellere Konvergenz reduziert.Das übergeordnete Ziel der Indoor-Mesh-Sicherheit besteht in folgenden Bereichen:Konfiguration ohne Benutzereingriff für die Bereitstellung von Sicherheit.Datenschutz und Authentifizierung für Daten-Frames.Gegenseitige Authentifizierung zwischen Netzwerk und Knoten.Verwendung von Standard-EAP-Methoden für die Authentifizierung von Indoor-Mesh-AP-Knoten.Entkopplung von LWAPP- und Indoor-Mesh-Sicherheit.Die Erkennungs-, Routing- und Synchronisierungsmechanismen wurden von der aktuellen Architektur erweitert, um die erforderlichen Elemente zur Unterstützung der neuen Sicherheitsprotokolle aufzunehmen.APs mit Innenvernetzung erkennen andere Mesh-APs, indem sie nach grundlosen Nachbaraktualisierungen von anderen Mesh-APs suchen und diese abhören. Alle mit dem Netzwerk verbundenen RAPs oder Indoor-MAPs geben in ihren NEIGH_UPD-Frames (ähnlich wie 802.11-Beacon-Frames) wichtige Sicherheitsparameter an.Nach Abschluss dieser Phase wird eine logische Verbindung zwischen einem Indoor-Mesh-AP und dem Root-AP hergestellt.
- **WCS-Erweiterungen**Indoor Mesh Alarme wurden hinzugefügt.In Indoor Mesh Reports können die Hop-Anzahl, die schlechteste SNR usw. angezeigt werden.Der Verbindungstest (Parent-to-Child, Child-to-Parent) kann zwischen den Knoten ausgeführt werden, wodurch sehr intelligente Informationen angezeigt werden.Die angezeigten AP-Informationen sind viel mehr als die vorherigen.Man hat die Möglichkeit, auch die potenziellen Nachbarn anzuzeigen.Die Statusüberwachung wird verbessert und der Zugriff wird benutzerfreundlicher.

Unterstützte Hardware und Software

Für ein Indoor-Mesh sind mindestens Hardware und Software erforderlich:

- Die Cisco LWAPP APs AIR-LAP1242AG-A-K9 und AIR-LAP1131AG-A-K9 unterstützen die Konfiguration von Mesh-Innenöffnungen.
- Die Mesh Release 2 Software von Cisco unterstützt Enterprise Mesh (Indoor- und Outdoor-Produkte). Diese kann nur auf Cisco Controller, Cisco 440x/210x und WiSMs installiert werden.
- Die Cisco Enterprise Mesh Release 2 Software kann von Cisco.com heruntergeladen werden.

Innenbereich und Außenbereich

Dies sind einige der wichtigsten Unterschiede zwischen Innen- und Außenvermaschung:

	Innenvermasch	Außenvermasch
Umgebung	NUR für den Innenbereich, bewertet mit Hardware für Innenbereiche	NUR für den Außenbereich, robuste Hardware
Hardware	AP für Innenbereiche	AP für

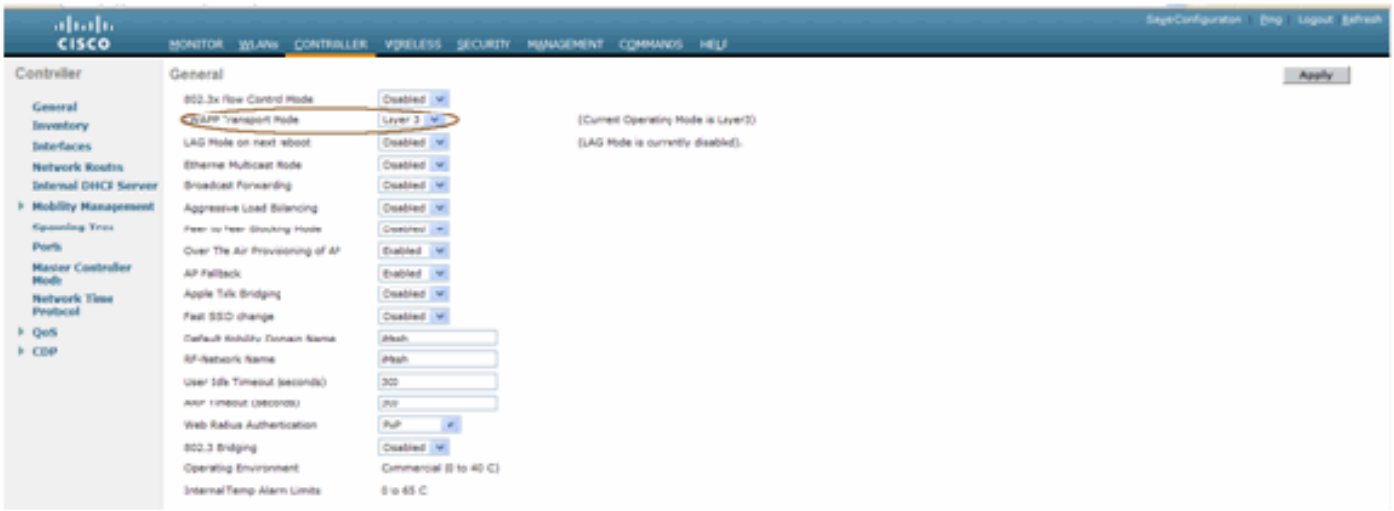
	mit LAP1242 und LAP1131AG	Außenbereiche mit LAP15xx und LAP152x
Leistungsstufen	2,4 GHz:20 dBm 5,8 GHz:17 dBm	2,4 GHz:28 dBm 5,8 GHz:28 dBm
Zellengröße	ca. 30 m	ca. 300 m
Implementierungshöhe	3 m vom Boden entfernt	10 bis 15 m vom Boden entfernt

Konfiguration

Lesen Sie den Leitfaden sorgfältig durch, bevor Sie mit der Implementierung beginnen, insbesondere wenn Sie neue Hardware erhalten haben.

Controller-L3-Modus

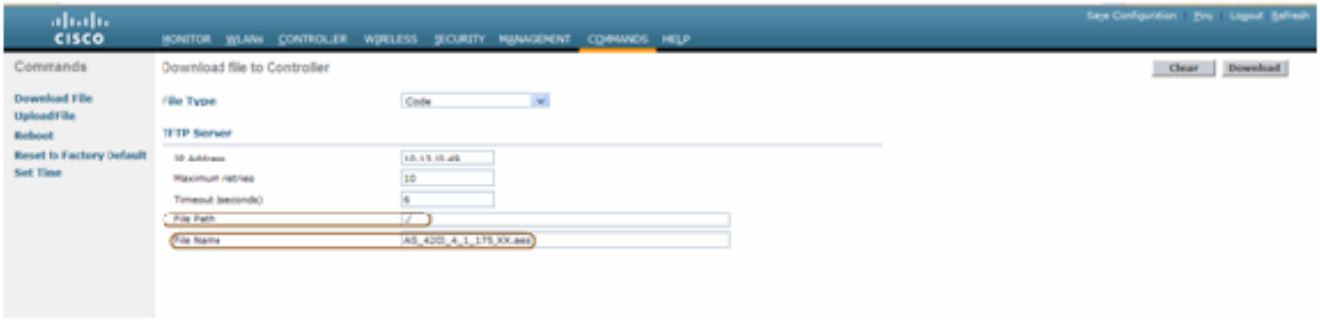
Indoor Mesh-APs können als L3-Netzwerk bereitgestellt werden.



Aktualisieren des Controllers auf den neuesten Code

Führen Sie diese Schritte aus:

1. Um Mesh Release 2 in einem Indoor Mesh-Netzwerk zu aktualisieren, muss Ihr Netzwerk auf Version 4.1.185.0 oder Mesh Release1 ausgeführt werden, verfügbar auf Cisco.com.
2. Laden Sie den aktuellen Code für den Controller auf Ihren TFTP-Server herunter. Klicken Sie in der Benutzeroberfläche des Controllers auf **Befehle > Datei herunterladen**.
3. Wählen Sie den Dateityp als **Code aus**, und geben Sie die IP-Adresse Ihres TFTP-Servers an. Definieren Sie den Pfad und den Namen der Datei.



Hinweis: Verwenden Sie den TFTP-Server, der Datenübertragungen mit einer Dateigröße von mehr als 32 MB unterstützt. Beispiel: **tftpd32**. Legen Sie unter Dateipfad **"./"** wie dargestellt fest.

4. Wenn Sie die Installation der neuen Firmware abgeschlossen haben, überprüfen Sie mithilfe des Befehls **show sysinfo** in der CLI, ob die neue Firmware installiert ist.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

Hinweis: Cisco bietet offiziell keine Unterstützung für Downgrades für Controller.

MAC-Adresse

MAC-Filterung ist obligatorisch. Diese Funktion hat die Cisco Indoor Mesh-Lösung zu einer echten Zero Touch-Lösung gemacht. Im Gegensatz zu den vorherigen Versionen verfügt der Mesh-Bildschirm nicht mehr über die MAC-Filtering-Option.

Hinweis: Die MAC-Filterung ist standardmäßig aktiviert.

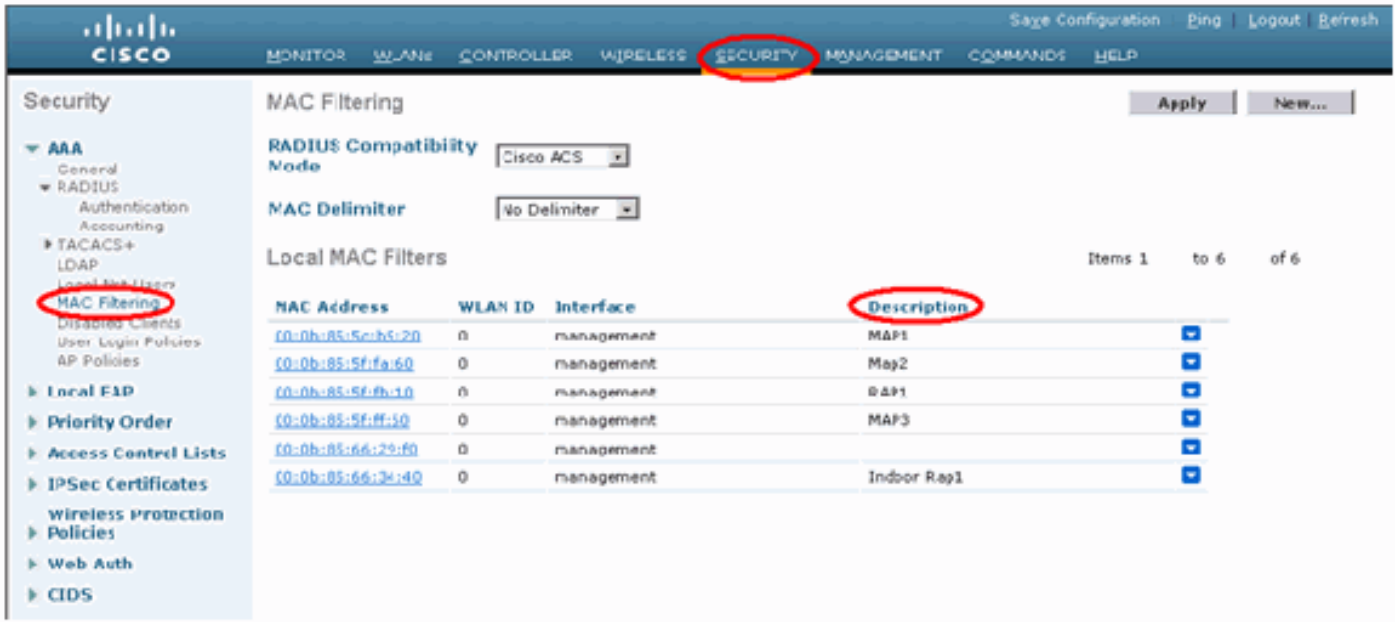
Aufzeichnen der MAC-Adresse in den Radios

Zeichnen Sie in einer Textdatei die MAC-Adressen aller in Ihrem Netzwerk bereitgestellten Mesh-AP-Funkmodule auf. Die MAC-Adresse befindet sich auf der Rückseite der APs. Dies hilft Ihnen bei zukünftigen Tests, da die meisten CLI-Befehle die Eingabe der MAC-Adresse bzw. der MAC-Namen der Access Points mit dem Befehl erfordern. Sie können den Namen der APs auch in etwas leichter merkbares ändern, z. B. "Building number-pod number-AP type: die letzten vier MAC-Adressen Hexadezimalzeichen."

Geben Sie die MAC-Adresse und die Namen der Funkmodule im Controller ein.

Der Cisco Controller unterhält eine MAC-Adressliste für die interne AP-Autorisierung. Der Controller reagiert nur auf Erkennungsanfragen von den Funkmodulen in Innenräumen, die in der Autorisierungsliste aufgeführt sind. Geben Sie die MAC-Adressen aller Funkmodule ein, die Sie im Netzwerk des Controllers verwenden.

Gehen Sie auf der GUI-Schnittstelle des Controllers zu **Sicherheit**, und klicken Sie links im Bildschirm auf **MAC-Filterung**. Klicken Sie auf **Neu**, um die MAC-Adressen wie hier gezeigt einzugeben:



Geben Sie außerdem die Namen der Funkmodule unter **Beschreibung** ein (z. B. Standort, AP-Nummer usw.). Eine Beschreibung kann auch dort verwendet werden, wo die Radios installiert wurden, um jederzeit leicht zu verweisen.

MAC-Filterung aktivieren

MAC-Filterung ist standardmäßig aktiviert.

Auf derselben Seite können Sie auch den Sicherheitsmodus als EAP oder PSK auswählen.

Verwenden Sie an der GUI-Schnittstelle des Switches den folgenden Pfad:

GUI-Schnittstellenpfad: **Wireless > Innenbereich**

Der Sicherheitsmodus kann NUR mit dem folgenden Befehl in der CLI aktiviert werden:

```
(Cisco Controller) > show network
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

L3 Indoor Mesh-Bereitstellung

Bei einem L3 Indoor Mesh Network konfigurieren Sie die IP-Adressen für die Funkmodule, wenn Sie den (internen oder externen) DHCP-Server nicht verwenden möchten.

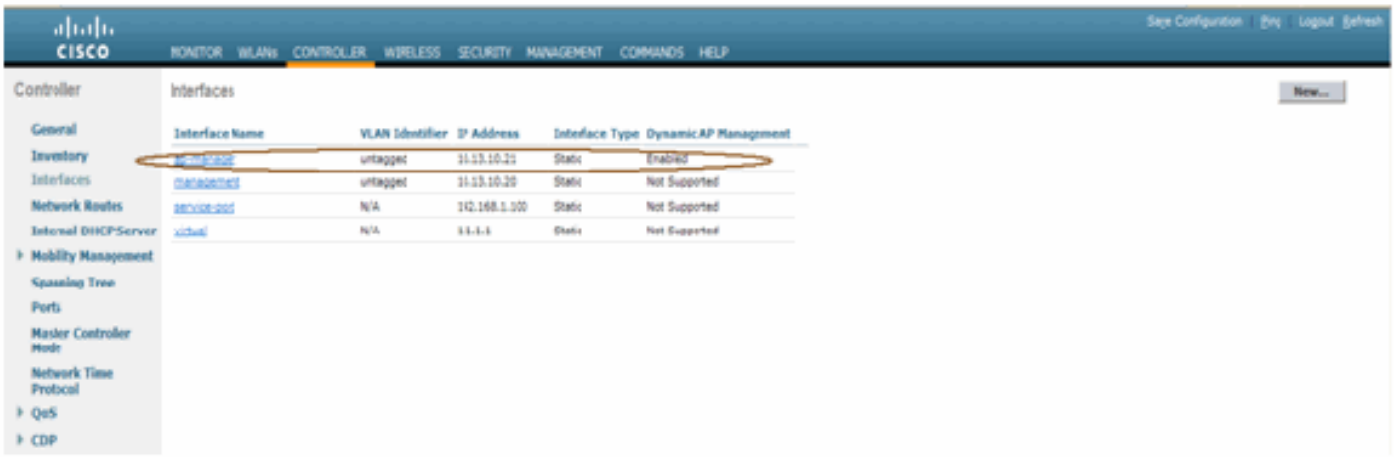
Wenn Sie für ein L3-Indoor-Mesh-Netzwerk einen DHCP-Server verwenden möchten, konfigurieren Sie den Controller im L3-Modus. Speichern Sie die Konfiguration, und starten Sie den Controller neu. Stellen Sie sicher, dass Sie Option 43 auf dem DHCP-Server konfigurieren. Nach dem Neustart des Controllers erhalten neu verbundene APs ihre IP-Adresse vom DHCP-Server.

Definieren von Schnittstellen im Controller

AP-Manager

Für eine L3-Bereitstellung müssen Sie den **AP-Manager** definieren. Der AP Manager fungiert als Quell-IP-Adresse für die Kommunikation zwischen dem Controller und den APs.

Pfad: **Controller > Schnittstellen > ap-manager > bearbeiten**.



Der **AP-Manager-**Schnittstelle sollte eine IP-Adresse im gleichen Subnetz und VLAN zugewiesen werden wie Ihrer Verwaltungsschnittstelle.

Funkrollen

Diese Lösung bietet zwei primäre Funkrollen:

- Root Access Point (RAP) - Das Funkmodul, mit dem Sie (über Switch) eine Verbindung zum Controller herstellen möchten, übernimmt die Rolle eines RAP. Die RAPs verfügen über eine kabelgebundene, LWAPP-fähige Verbindung zum Controller. Ein RAP ist ein übergeordneter Knoten zu einem Bridging- oder Indoor-Mesh-Netzwerk. Ein Controller kann über einen oder mehrere RAPs verfügen, von denen jeder ein und dasselbe oder verschiedene Wireless-Netzwerke überträgt. Aus Redundanzgründen können mehrere RAPs für dasselbe Indoor-Mesh-Netzwerk vorhanden sein.
- Indoor Mesh Access Point (MAP) - Das Funkmodul ohne Kabelverbindung zum Controller übernimmt die Rolle eines Indoor Mesh Access Points. Dieser AP wurde früher als Pole Top AP bezeichnet. MAPs verfügen über eine Wireless-Verbindung (über die Backhaul-Schnittstelle) zu möglicherweise anderen MAPs und schließlich zu einem RAP und damit zum Controller. MAPs können auch über eine verdrahtete Ethernet-Verbindung mit einem LAN verfügen und als Bridge-Endpunkt für dieses LAN dienen (über eine P2P- oder P2MP-Verbindung). Dies kann gleichzeitig erfolgen, wenn die Konfiguration ordnungsgemäß als Ethernet Bridge erfolgt. MAPs-Service-Clients im Band werden nicht für die Backhaul-Schnittstelle verwendet.

Der Standardmodus für einen AP ist MAP.

Hinweis: Die Funkrollen können über GUI oder CLI festgelegt werden. Die APs werden nach der Rollenänderung neu gestartet.

Hinweis: Sie können die Funkrollen eines Access Points mithilfe der Controller-CLI vorkonfigurieren, sofern der Access Point physisch mit dem Switch verbunden ist. Sie können auch den Access Point auf dem Switch als RAP oder MAP anzeigen.

```
(Cisco Controller) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Bridge-Gruppen-Name

Bridge-Gruppen-Namen (BGN) steuern die Zuordnung der APs. BGNs können die Funkmodule logisch gruppieren, um zu verhindern, dass zwei Netzwerke auf demselben Kanal miteinander kommunizieren. Diese Einstellung ist auch dann nützlich, wenn Ihr Netzwerk im gleichen Sektor (Bereich) über mehr als einen RAP verfügt. Der BGN ist eine Zeichenfolge mit maximal zehn Zeichen.

Ein werkseitig eingestellter Bridge-Gruppenname wird in der Herstellungsphase zugewiesen (NULL VALUE). Es ist für Sie nicht sichtbar. Daher können die Funkmodule auch ohne definierten BGN dem Netzwerk beitreten. Wenn Ihr Netzwerk im gleichen Sektor über zwei RAPs verfügt (für mehr Kapazität), wird empfohlen, die beiden RAPs mit demselben BGN, jedoch auf unterschiedlichen Kanälen zu konfigurieren.

Hinweis: Der Bridge-Gruppenname kann über die CLI und GUI des Controllers festgelegt werden.

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Nach der Konfiguration des BGN wird der Access Point zurückgesetzt.

Hinweis: Der BGN sollte in einem Live-Netzwerk sehr sorgfältig konfiguriert werden. Sie sollten immer vom am weitesten entfernten Knoten (dem letzten Knoten) starten und sich zum RAP bewegen. Wenn Sie das BGN irgendwo in der Mitte des Multihop konfigurieren, werden die Knoten über diesen Punkt hinaus verworfen, da diese Knoten einen anderen BGN (alten BGN) haben.

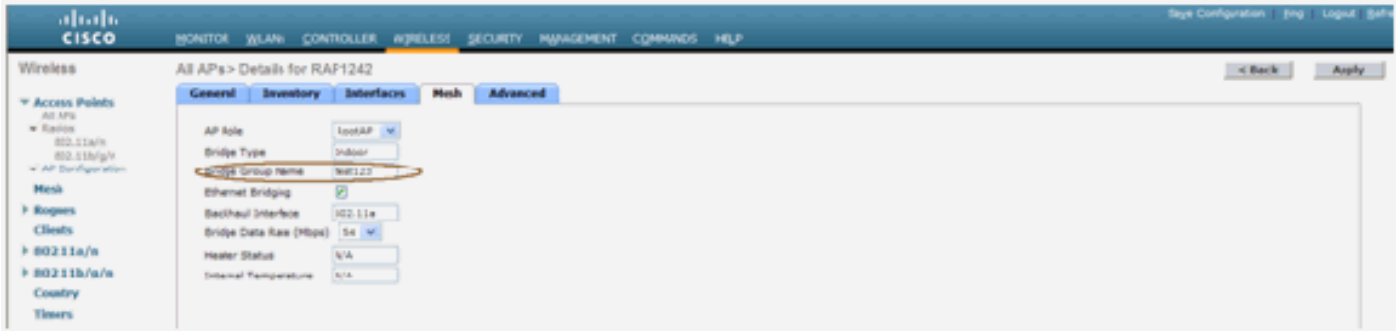
Sie können den BGN überprüfen, indem Sie den folgenden CLI-Befehl eingeben:

```
(Cisco Controller) > show ap config general
```

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB    802.11a:-A3
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:18:74:fa:7d:1f
IP Address Configuration......................... DHCP
IP Address....................................... 10.13.13.11
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch........................... 
Tertiary Cisco Switch............................ 
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
AP Role ......................................... RootAP
Ethernet Bridging ............................... Enabled
Bridge GroupName ................................ test123
Public Safety ..................................  Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.175.19
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation........... Disabled
Console Login Name............................... 
Console Login State.............................. Unknown
AP Up Time....................................... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time................................. 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time............................... Sun Aug 19 11:59:07 2007

Join Taken Time.................................. 0 days, 00 h 00 m 24 s
Ethernet Port Duplex............................. Unknown
Ethernet Port Speed.............................. Unknown
```

Sie können den BGN auch mithilfe der Controller-GUI konfigurieren oder überprüfen:

Pfad: **Wireless > Alle APs > Details**.



Sie sehen, dass die Umgebungsinformationen des Access Points auch mit dieser neuen Version angezeigt werden.

Sicherheitskonfiguration

Der standardmäßige Indoor-Mesh-Sicherheitsmodus ist EAP. Das bedeutet, dass die MAPs nur dann gemeinsam verwendet werden, wenn Sie diese Parameter auf Ihrem Controller konfigurieren:

Indoor Mesh EAP-Konfigurations-CLI

```
(Cisco Controller) >config mesh local-auth enable

 enable Local Auth

(Cisco Controller) >config advanced eap ?

identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index      Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

Wenn Sie im PSK-Modus bleiben müssen, verwenden Sie diesen Befehl, um wieder in den PSK-Modus zu wechseln:

```
(Cisco Controller) >config mesh security psk ?

(Cisco Controller) >config mesh security psk

 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)n
```

Indoor Mesh EAP zeigt Befehle an

Im EAP-Modus können Sie die folgenden **show**-Befehle überprüfen, um die MAP-Authentifizierung zu überprüfen:

```
(Cisco Controller) >show network

RF Network Name............................... jaggi123
Web Mode...................................... Disable
Secure Web Mode............................... Enable
Secure Shell (ssh)............................ Enable
Telnet........................................ Enable
Ethernet Multicast Mode....................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode....................... Disable
User Idle Timeout............................. 300 seconds
ARP Idle Timeout.............................. 300 seconds
ARP Unicast Mode.............................. Disabled
Cisco AP Default Master....................... Disable
Mgmt Via Wireless Interface................... Enable
Mgmt Via Dynamic Interface.................... Disable
Bridge MAC filter Config...................... Disable
Bridge Security Mode.......................... EAP  otherwise PSK
Mesh Multicast Mode........................... 802.11b/g/n
Mesh Full Sector DFS.......................... Enable
Over The Air Provisioning of AP's............. Enable
Mobile Peer to Peer Blocking.................. Disable
AP Fallback .................................. Enable
Web Auth Redirect Ports ...................... 80
--More-- or (q)uit
Fast SSID Change ............................. Disabled
802.3 Bridging ............................... Disable
```

```
(Cisco Controller) >show wlan 0
```

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500L1EAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ........................................... Disabled
   IP Security Passthru........................... Disabled
   Web Based Authentication....................... Disabled
   Web-Passthrough................................ Disabled
   Conditional Web Redirect....................... Disabled
   Auto Anchor.................................... Disabled
--More-- or (q)uit
   H-REAP Local Switching......................... Disabled
   Infrastructure MFP protection.................. Enabled (Global Infrastructure MFP Disabled)
   Client MFP..................................... Optional
   Tkip MIC Countermeasure Hold-down Timer........ 60

 Mobility Anchor List
 WLAN ID       IP Address         Status
```

(Cisco Controller) >**show local-auth config**

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 1
EAP-Request Max Retries.................... 2
```

```
(Cisco Controller) >show advanced eap
```

Indoor Mesh EAP-Debug-Befehle

Verwenden Sie zum Debuggen von EAP-Modusproblemen die folgenden Befehle im Controller:

```
(Cisco Controller) >debug dot1x all enable

(Cisco Controller) >debug aaa all enable
```

Installation

Voraussetzungen

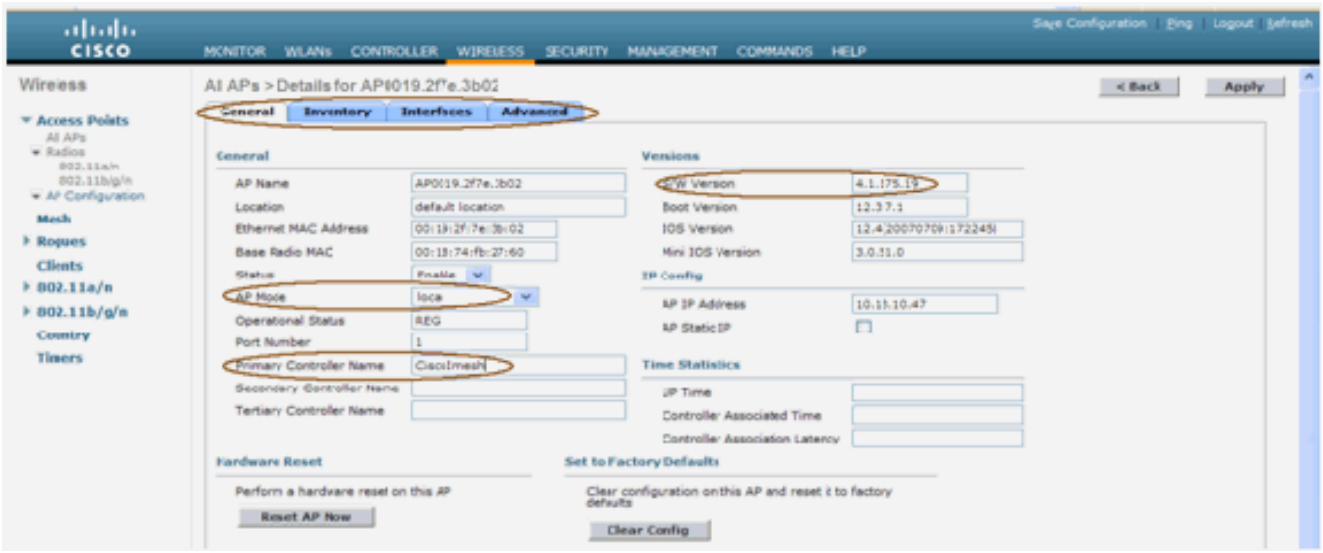
Der Controller muss die empfohlene Codeversion ausführen. Klicken Sie auf **Monitor**, um die Softwareversion zu überprüfen. Dasselbe kann auch über CLI überprüft werden.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

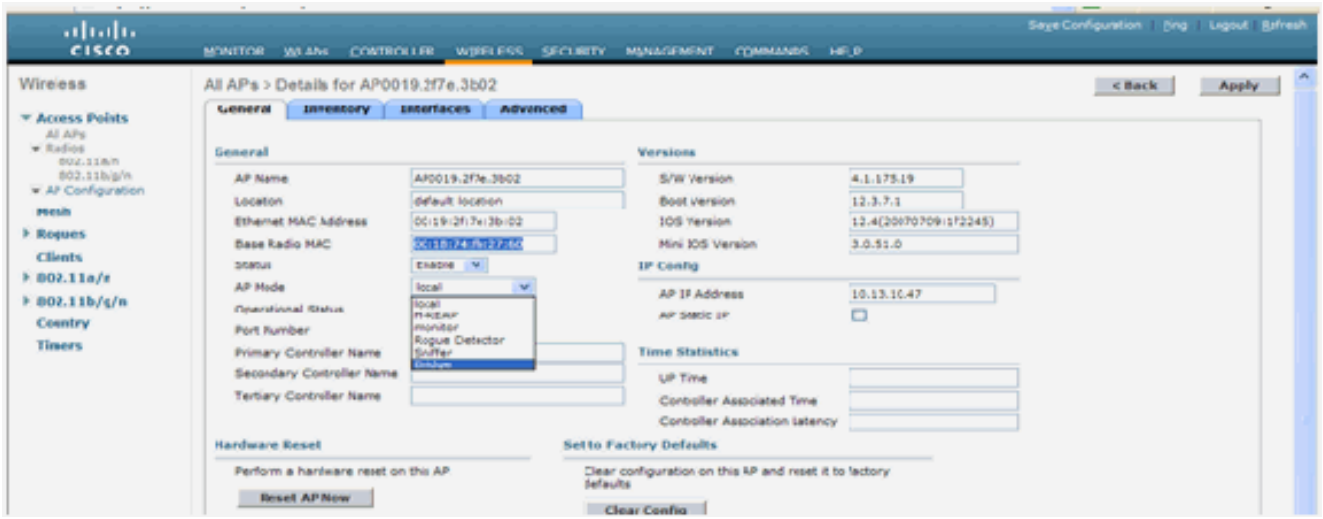
Systeme wie der DHCP-Server, der ACS-Server und der WCS-Server sollten erreichbar sein.

Installation

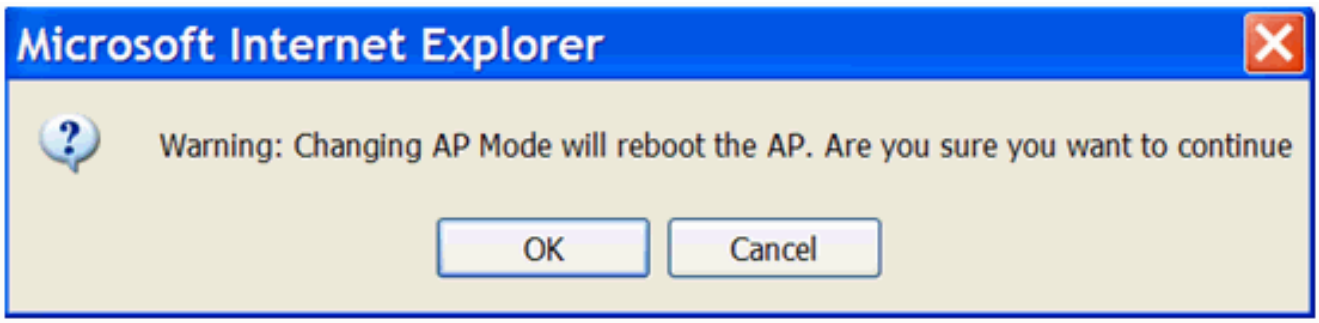
1. Verbinden Sie alle LAPs (1131AG/1242AG) mit einem Layer-3-Netzwerk im gleichen Subnetz wie die Management-IP-Adresse. Alle APs werden dem Controller als APs im lokalen Modus hinzugefügt. In diesem Modus primieren Sie die Access Points mit dem Namen des primären Controllers, dem Namen des sekundären Controllers und einem Tertiären
   Controller.



2. Erfassen Sie die MAC-Adresse des Access Points für Basisfunkmodule (z. B. 00:18:74: fb: 27:60).
3. Fügen Sie die MAC-Adresse des AP hinzu, damit der Access Point im Bridge-Modus verbunden wird.
4. Klicken Sie auf **Sicherheit** > **MAC-Filterung** > **Neu**.
5. Fügen Sie die kopierte MAC-Adresse hinzu, und nennen Sie die APs in der MAC-Filterliste und in der AP-Liste.
6. Wählen Sie **Bridge** aus der **AP Mode**-Liste aus.



7. Sie werden aufgefordert, die Bestätigung zu erteilen, da der Access Point neu gestartet wird.



8. Der Access Point wird neu gestartet, und der Controller wird im Bridge-Modus angeschlossen. Das neue Fenster des Access Points verfügt über eine zusätzliche Registerkarte: MESH. Klicken Sie auf die Registerkarte **MESH**, um die Rolle, den Bridge-Typ, den Namen der Bridge-Gruppe, das Ethernet-Bridging, die Backhaul-Schnittstelle, die

Bridge-Datenrate usw. zu überprüfen.

9. Rufen Sie in diesem Fenster die Liste der AP-Rollen auf, und wählen Sie die entsprechende Rolle aus. In diesem Fall ist die Rolle standardmäßig ein MAP.Der Bridge-Gruppenname ist standardmäßig leer.Die Back-Haul-Schnittstelle ist 802.11a.Die Bridge-Datenrate (Backhaul-Datenrate) beträgt 24 Mbit/s.
10. Verbinden Sie den als RAP gewünschten Access Point mit dem Controller. Stellen Sie die Funkmodule (MAPs) an den gewünschten Stellen bereit. Schalten Sie die Funkmodule ein. Sie sollten alle Funkmodule auf dem Controller sehen können.

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name             Slots  AP Model             Ethernet MAC       Location          Port  Country
-----------------   -----  -------------------  -----------------  ----------------  ----  -------
RAP1242             2      AIR-LAP1242AG-A-K9   00:18:74:fa:7d:1f  default location  1     US
LAP1242-1           2      AIR-LAP1242AG-A-K9   00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2           2      AIR-LAP1242AG-A-K9   00:14:1b:59:07:af  default location  1     US
```

11. Versuchen Sie, Bedingungen in Sichtlinie zwischen den Knoten zu haben. Wenn keine Sichtlinie vorhanden ist, sollten Sie Fresnel-Zonenfreigaben erstellen, um die Bedingungen in der Nähe des Standorts zu erhalten.
12. Wenn mehrere Controller mit demselben Indoor-Mesh-Netzwerk verbunden sind, müssen Sie für jeden Knoten den Namen des primären Controllers angeben. Andernfalls wird der Controller, der zuerst angezeigt wird, als primäres Gerät betrachtet.

Konfiguration von Stromversorgung und Kanal

Der Backhaul-Kanal kann auf einem RAP konfiguriert werden. MAPs werden auf den RAP-Kanal abgestimmt. Der lokale Zugriff kann für MAPs unabhängig konfiguriert werden.

Folgen Sie der Switch-GUI: **Wireless > 802.11a-Funkmodul > Konfigurieren**.

Hinweis: Der Tx-Standardstrompegel für das Backhaul ist der höchste Leistungsgrad (Stufe 1), und das Radio Resource Management (RRM) ist standardmäßig deaktiviert.

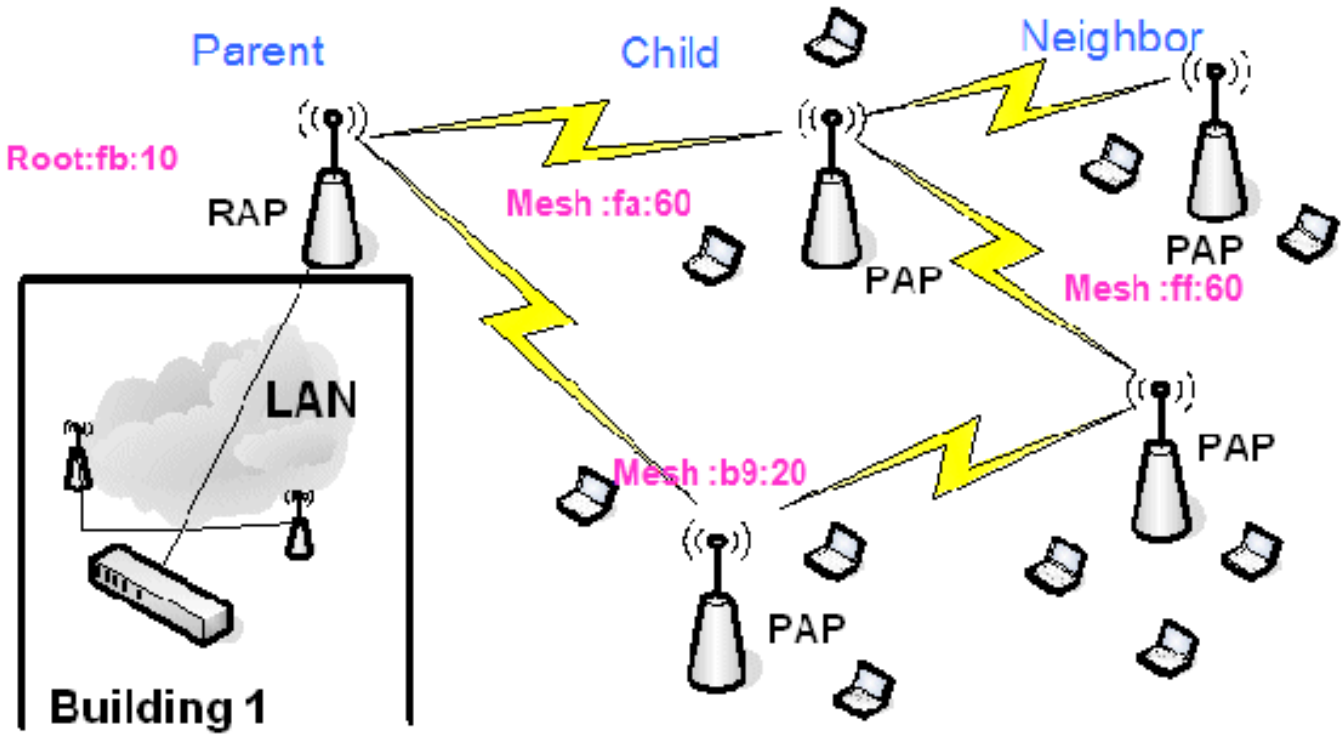
Wenn Sie RAPs zusammenfassen, empfehlen wir die Verwendung alternativer benachbarter Kanäle auf jedem RAP. Dies reduziert die Interferenz mit Kanälen.

RF-Prüfung

In einem Indoor-Mesh-Netzwerk müssen wir die Parent-Child-Beziehung zwischen den Knoten überprüfen. **Hop** ist eine Wireless-Verbindung zwischen den beiden Funkmodulen. Die Beziehung zwischen Eltern und Kind ändert sich, wenn Sie das Netzwerk durchlaufen. Das hängt davon ab, wo Sie sich im Indoor-Mesh-Netzwerk befinden.

Das Funkmodul, das sich in einer Wireless-Verbindung (Hop) näher am Controller befindet, ist eine **Parent** des Funkmoduls auf der anderen Seite des Hop. In einem Multiple-Hop-System gibt es eine Baumstruktur, bei der der mit dem Controller verbundene Knoten ein RAP (**Parent**) ist. Der direkte Knoten auf der anderen Seite des ersten Hop ist ein **Child**, und nachfolgende Knoten im zweiten Hop sind die **Nachbarn** für diesen bestimmten Parent.

Abbildung 1: Zwei-Hop-Netzwerke



In Abbildung 1 werden die Namen der Access Points aus Gründen der Einfachheit genannt. Im nächsten Screenshot wird das **RAP(fb:10)** untersucht. Dieser Knoten kann die Indoor Mesh Access Points **(fa:60 & b9:20)** als untergeordnete Access Points und **MAP ff:60 als Nachbar** sehen (in der eigentlichen Bereitstellung).

Folgen Sie der GUI-Schnittstelle des Switches: **Wireless > Alle APs > Rap1 > Neighbor Info**.

Stellen Sie sicher, dass die Beziehung zwischen Eltern und Kindern korrekt für Ihr Indoor Mesh Network eingerichtet und aufrechterhalten wird.

Überprüfen der Verbindungen

show Mesh ist ein informativer Befehl zur Überprüfung der Interkonnektivität in Ihrem Netzwerk.

Sie müssen diese Befehle an jedem Knoten (AP) mithilfe der Controller-CLI geben und die Ergebnisse in einer Word- oder Textdatei auf die Upload-Site hochladen.

```
(Cisco Controller) >show mesh ?

env             Show mesh environment.
neigh           Show AP neigh list.
path            Show AP path.
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

Wählen Sie in Ihrem Indoor Mesh-Netzwerk eine Multiple Hop-Verbindung aus, und geben Sie diese Befehle ab dem RAP aus. Laden Sie das Ergebnis der Befehle auf die Upload-Site hoch.

Im nächsten Abschnitt wurden alle diese Befehle für das Two-Hop Indoor Mesh Network ausgegeben (siehe Abbildung 1).

Indoor Mesh Path anzeigen

Dieser Befehl zeigt die MAC-Adressen, die Funkrollen der Knoten, Signal-Rauschverhältnisse in dBs für Uplink/Downlink (SNRUp, SNRDown) und Link SNR in dB für einen bestimmten Pfad an.

```
(Cisco Controller) >show mesh path RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
RAP1242           is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-1           56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242             56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242           is a Root AP.
```

Indoor Mesh Neighbor-Zusammenfassung anzeigen

Dieser Befehl zeigt die MAC-Adressen, die Beziehungen zwischen Eltern und Kindern und die Uplink/Downlink-SNRs in dB an.

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

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      0      0        0        0x860    BEACON
LAP1242-1           56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242             56      43     46       31       0x86b    UPDATED NEIGH PARENT BEACON
```

Bis dahin sollten Sie die Beziehungen zwischen den Knoten Ihres Netzwerks sehen und die RF-Konnektivität überprüfen können, indem Sie die SNR-Werte für jede Verbindung anzeigen.

Zugriffssicherheit der AP-Konsole

Diese Funktion erhöht die Sicherheit des Konsolenzugriffs des Access Points. Für die Verwendung dieser Funktion ist ein Konsolenkabel für den AP erforderlich.

Diese werden unterstützt:

- Eine CLI, die die Kombination aus Benutzer-ID und Kennwort an den angegebenen Access Point
  überträgt:

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- Ein CLI-Befehl zum Übertragen der Kombination aus Benutzername und Kennwort an alle APs, die für den Controller registriert
  sind:

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

Mit diesen Befehlen wird die vom Controller gesendete Kombination aus Benutzer- und Kennwort während des erneuten Ladens auf die APs konstant gehalten. Wenn ein Access Point vom Controller gelöscht wird, gibt es keinen Sicherheitszugriffsmodus. Der AP generiert ein SNMP-Trap mit erfolgreicher Anmeldung. Der AP generiert außerdem ein SNMP-Trap bei einem Konsolen-Anmeldefehler drei Mal hintereinander.

Ethernet-Bridging

Aus Sicherheitsgründen ist der Ethernet-Port auf den MAPs standardmäßig deaktiviert. Sie kann nur aktiviert werden, indem Ethernet-Bridging auf dem RAP und den entsprechenden MAPs konfiguriert wird.

Daher muss Ethernet Bridging für zwei Szenarien aktiviert werden:

- Wenn Sie die Indoor Mesh-Knoten als Bridges verwenden möchten.
- Wenn Sie ein Ethernet-Gerät (z. B. PC/Laptop, Videokamera usw.) an den MAP anschließen möchten, verwenden Sie dessen Ethernet-Port.

Pfad: **Wireless** > Klicken Sie auf einen beliebigen Access Point > **Mesh**.

Es gibt einen CLI-Befehl, mit dem der Abstand zwischen den Knoten, die die Bridging-Funktion ausführen, konfiguriert werden kann. Versuchen Sie, ein Ethernet-Gerät wie eine Videokamera an

jedem Hop anzuschließen, und sehen Sie die Leistung.

Erweiterung des Bridge-Gruppen-Namens

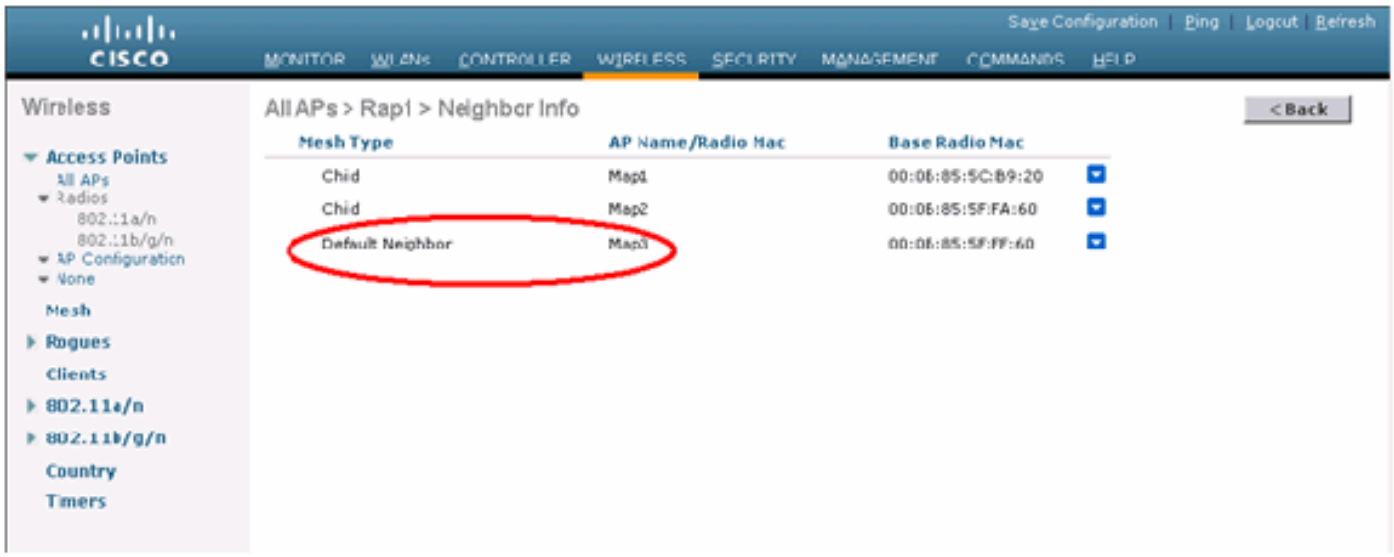
Es ist möglich, dass ein Access Point fälschlicherweise mit einem "Bridgegroupname" bereitgestellt wird, für den er nicht vorgesehen war. Je nach Netzwerkdesign ist dieser Access Point möglicherweise nicht in der Lage, den richtigen Sektor bzw. die richtige Struktur zu finden. Wenn sie einen kompatiblen Sektor nicht erreichen kann, kann sie festgefahren werden.

Um einen solchen stranded Access Point wiederherzustellen, wurde das Konzept des "default"-Bridgegroupnamens mit dem Code 3.2.xx.x eingeführt. Die Grundidee ist, dass ein Access Point, der mit seinem konfigurierten Bridgegroupnamen keine Verbindung zu einem anderen Access Point herstellen kann, versucht, eine Verbindung mit "default" (dem Wort) als bridgegroupname herzustellen. Alle Knoten, auf denen 3.2.xx.x und höher ausgeführt werden, akzeptieren andere Knoten mit diesem Bridgegroupname.

Diese Funktion kann auch helfen, einem laufenden Netzwerk einen neuen Knoten oder einen falschen konfigurierten Knoten hinzuzufügen.

Wenn Sie über ein laufendes Netzwerk verfügen, nehmen Sie einen vorkonfigurierten Access Point mit einem anderen BGN und stellen Sie sicher, dass dieser dem Netzwerk beitritt. Dieser Access Point wird im Controller mithilfe des "Standard"-BGN angezeigt, nachdem Sie seine MAC-Adresse im Controller hinzugefügt haben.

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
 linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



Der Access Point, der das Standard-BGN verwendet, kann als normaler Indoor Mesh Access Point fungieren, der Clients zuordnet und untergeordnete Indoor Mesh-Beziehungen aufbaut.

Wenn dieser AP mit dem Standard-BGN ein anderes übergeordnetes Element mit dem richtigen BGN findet, wird er zu diesem wechseln.

Protokolle - Nachrichten, Sys, AP und Trap

Nachrichtenprotokolle

Aktivieren Sie die Berichtsebene für Nachrichtenprotokolle. Geben Sie in der Controller-CLI den folgenden Befehl ein:

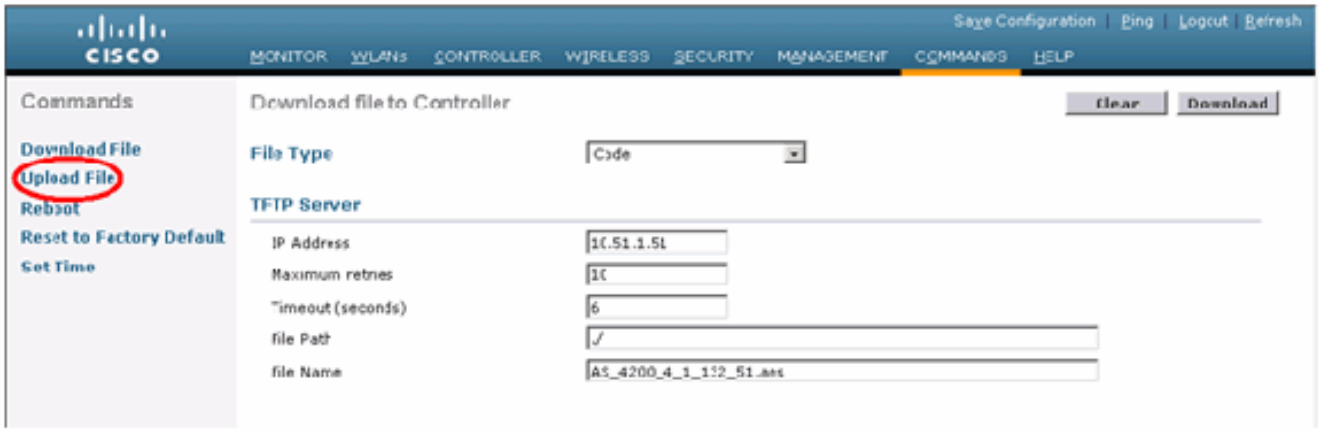
```
(Cisco Controller) >config msglog level ?

critical        Critical hardware or software Failure.
error           Non-Critical software error.
security        Authentication or security related error.
warning         Unexpected software events.
verbose         Significant system events.

(Cisco Controller) >config msglog level verbose
```

Führen Sie den folgenden Befehl aus der Controller-CLI aus, um Meldungsprotokolle anzuzeigen:

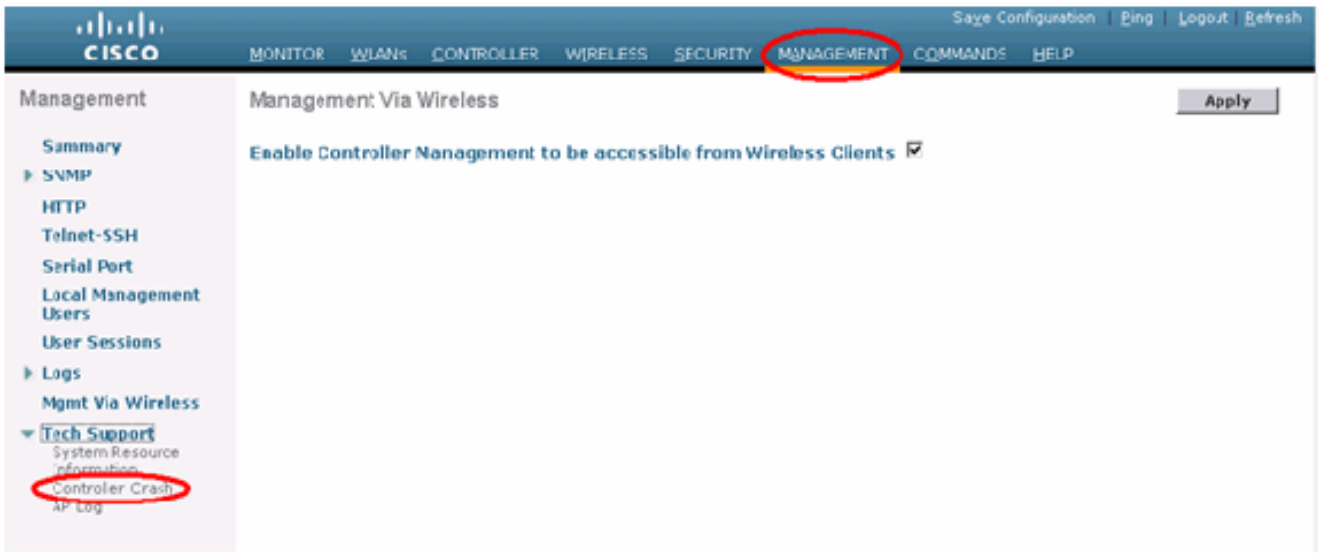
```
(Cisco Controller) >show msglog

Message Log Severity Level ..................... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul  8 06:12:02 2005  [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul  8 05:40:15 2005  [ERROR] spam_tmr.c 501: Did not receive hearbeat reply
 from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  8 05:38:40 2005  Previous message occurred 5 times
Fri Jul  8 05:33:54 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

Verwenden Sie zum Hochladen der Meldungsprotokolle die grafische Benutzeroberfläche des Controllers:

1. Klicken Sie auf **Befehle** > **Hochladen**.

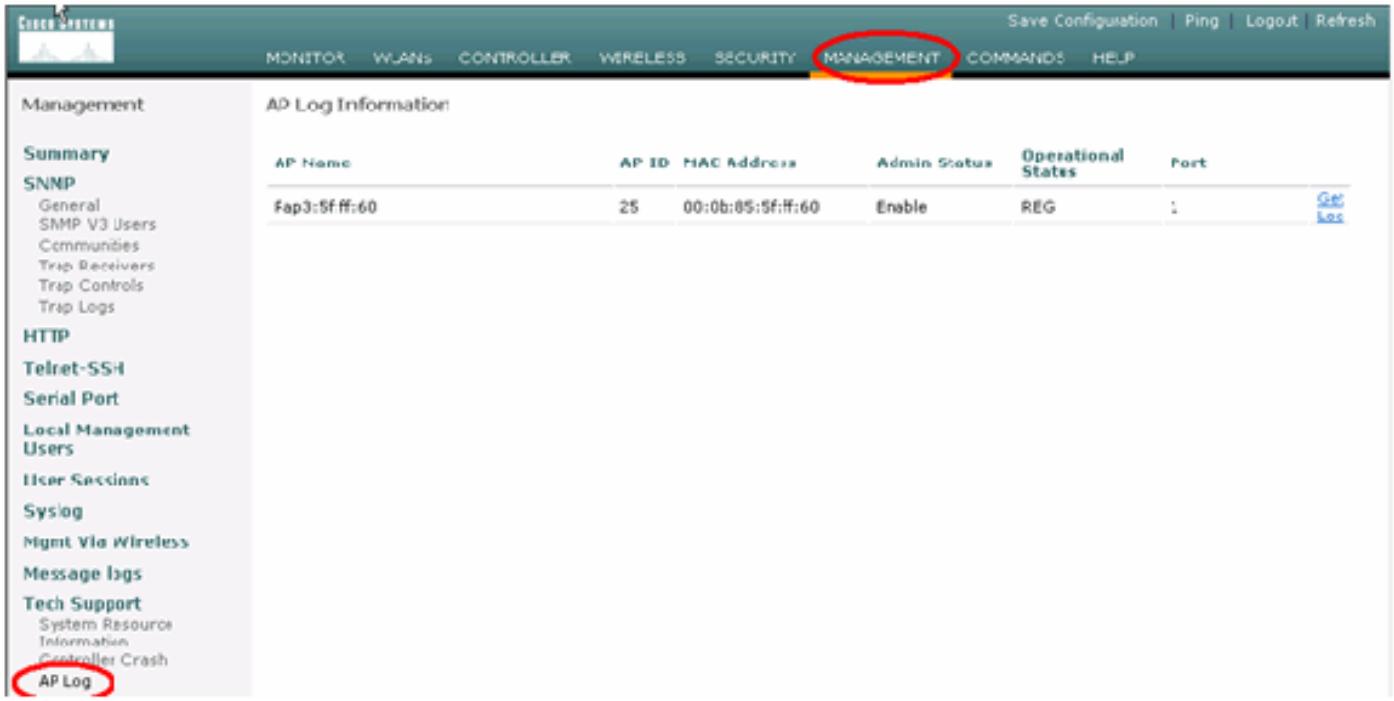


2. Geben Sie Ihre TFTP-Serverinformationen ein. Auf dieser Seite stehen Ihnen verschiedene Upload-Optionen zur Verfügung. Sie möchten, dass diese Dateien gesendet werden:NachrichtenprotokollEreignisprotokollTrap-ProtokollAbsturzdatei (falls vorhanden)Um nach Crash-Dateien zu suchen, klicken Sie auf **Management > Controller Crash**.



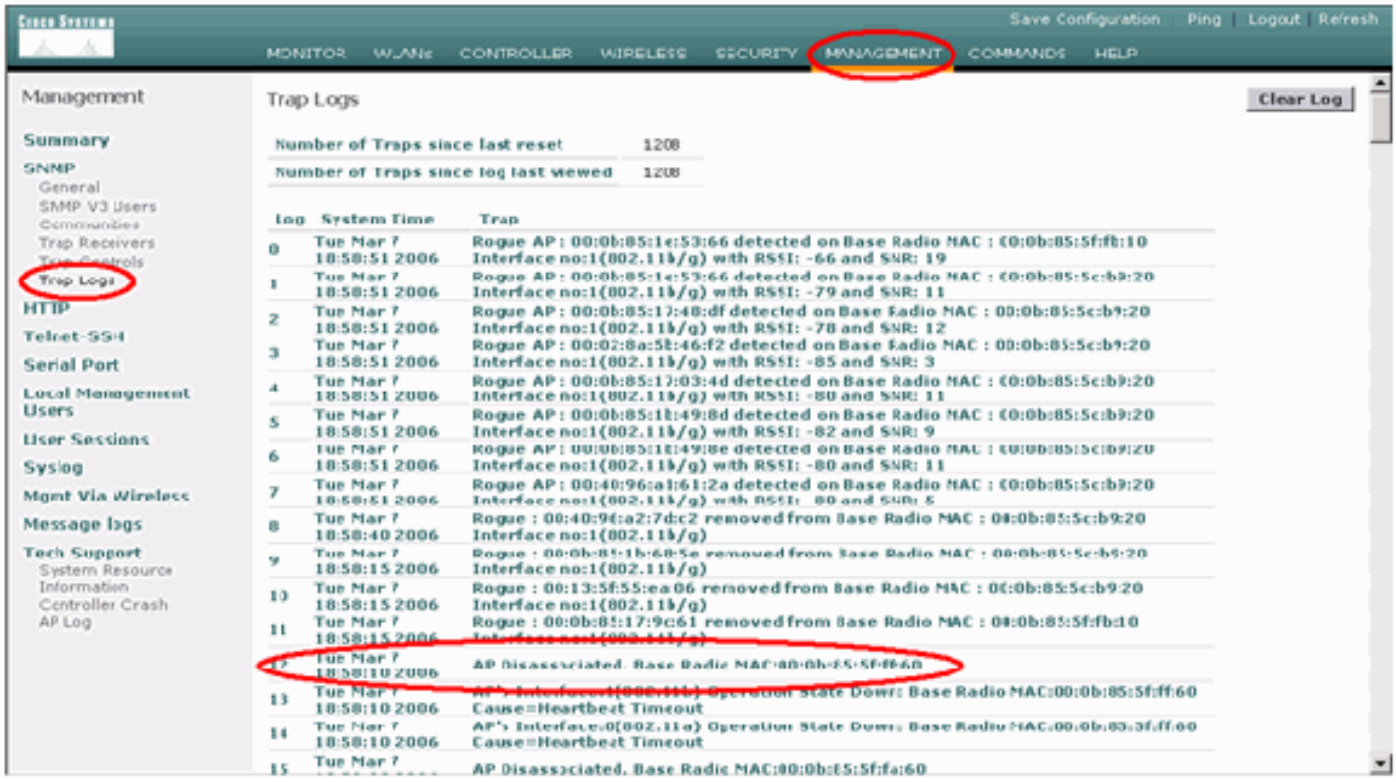
AP-Protokolle

Gehen Sie zu dieser GUI-Seite des Controllers, um die AP-Protokolle für Ihren lokalen Access Point zu überprüfen, falls vorhanden:



Trap-Protokolle

Rufen Sie diese GUI-Seite des Controllers auf, und überprüfen Sie die Trap-Protokolle:



Leistung

Startup Convergence-Test

Die Konvergenz ist die Zeit, die ein RAP/MAP benötigt, um eine stabile LWAPP-Verbindung mit einem WLAN-Controller herzustellen, beginnend mit dem Zeitpunkt, zu dem er das erste Mal hochgefahren wurde, wie hier aufgeführt:

Konvergenztest	Konvergenzzeit (min:sec)			
	RAP	MAP1	MAP2	MAP3
Image-Aktualisierung	2:34	3:50	5:11	6:38
Controller-Neustart	0:38	0:57	1:12	1:32
Einschalten des Mesh-Netzwerks in Innenräumen	2:44	3:57	5:04	6:09
RAP-Neustart	2:43	3:57	5:04	6:09
MAP-Rejoin		3:58	5:14	6:25
MAP-Änderung des übergeordneten Elements (gleicher Kanal)		0:38		

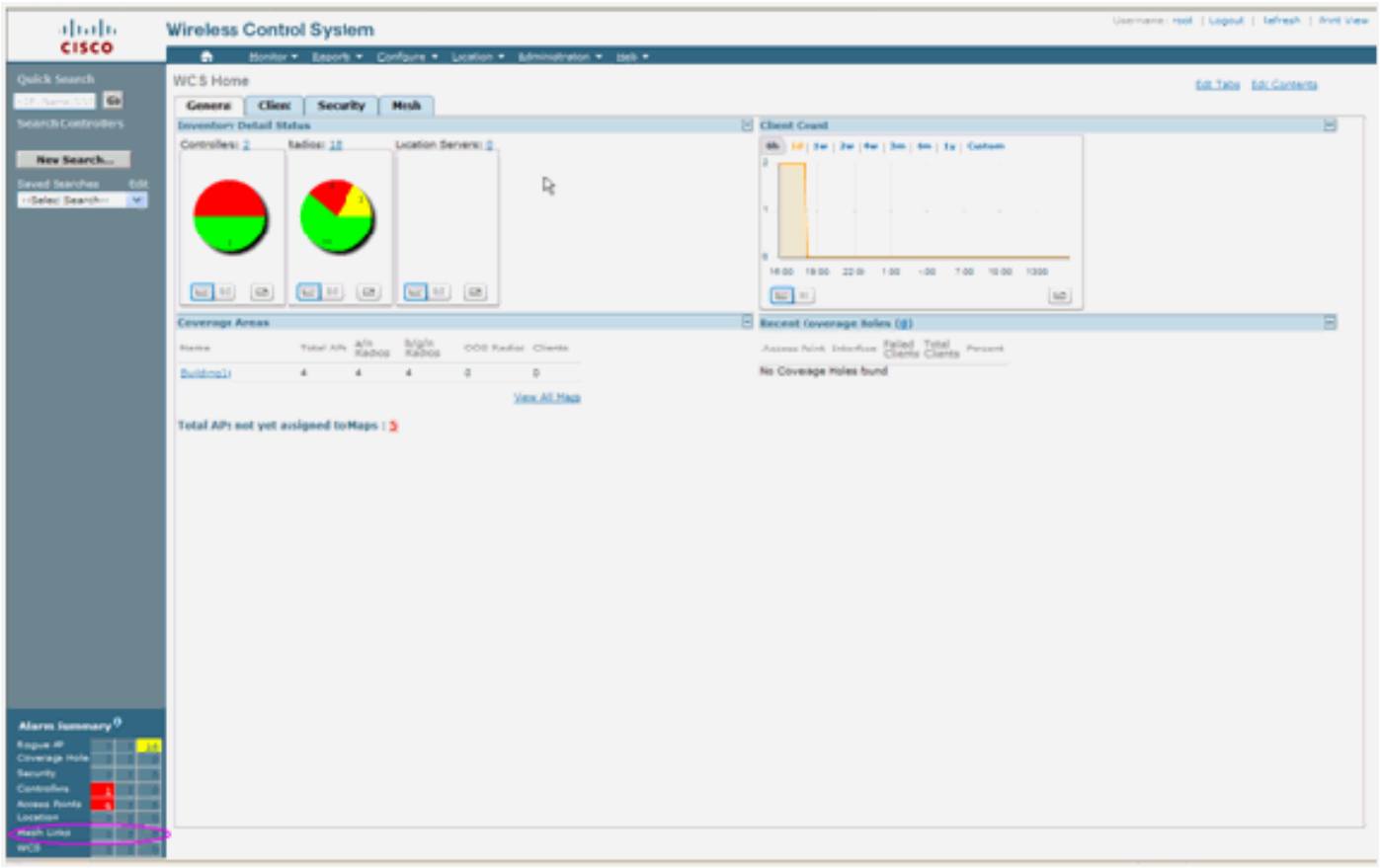
WCS

Indoor Mesh-Alarme

WCS generiert diese Alarme und Ereignisse im Zusammenhang mit dem Indoor Mesh-Netzwerk auf Basis der Traps des Controllers:

- Schlechter Link SNR
- Übergeordnet geändert
- Kind bewegt
- Häufig werden MAP-Änderungen übergeordnet
- Konsolenport-Ereignis
- MAC-Autorisierungsfehler
- Authentifizierungsfehler
- Untergeordnete übergeordnet

Klicken Sie auf **Vermaschte Links**. Es werden alle Alarme angezeigt, die sich auf Indoor-Mesh-Links beziehen.



Diese Alarme gelten für Indoor-Mesh-Links:

- Schlechte SNR-Verbindung - Dieser Alarm wird ausgelöst, wenn die SNR-Verbindung unter 12 db fällt. Der Benutzer kann diesen Schwellenwert nicht ändern. Wenn eine schlechte SNR-Funktion auf der Backhaul-Verbindung für Kind/Eltern erkannt wird, wird das Trap generiert. Das Trap enthält den SNR-Wert und die MAC-Adressen. Der Alarmschweregrad ist schwerwiegend. Das SNR-Verhältnis (Signal-Rausch) ist wichtig, da eine hohe Signalstärke für eine gute Empfängerleistung nicht ausreicht. Das eingehende Signal muss stärker sein als alle vorhandenen Geräusche oder Störungen. So ist es beispielsweise möglich, eine hohe Signalstärke zu haben und auch bei starker Interferenz oder hohem Rauschpegel eine schlechte Wireless-Leistung zu erzielen.
- Übergeordnet geändert - Dieser Alarm wird generiert, wenn das Kind zu einem anderen übergeordneten Element verschoben wird. Wenn das übergeordnete Element verloren geht, schließt sich das Kind einem anderen übergeordneten Element an, und das untergeordnete Element sendet ein Trap, das sowohl die MAC-Adressen des alten übergeordneten Elements als auch der neuen übergeordneten Person enthält. Alarmschweregrad: Informatorisch.
- Child Move (Untergeordnetes Verschieben) - Dieser Alarm wird generiert, wenn WCS ein Child Love-Feld erhält. Wenn der übergeordnete Access Point den Verlust eines untergeordneten Elements erkannte und nicht in der Lage ist, mit diesem untergeordneten Element zu kommunizieren, sendet er ein untergeordnetes Trap an WCS. Das Trap enthält die untergeordnete MAC-Adresse. Alarmschweregrad: Informatorisch.
- Häufig geänderte MAP-Eltern - Dieser Alarm wird generiert, wenn der Indoor Mesh AP seinen übergeordneten Access Point regelmäßig wechselt. Wenn der übergeordnete MAP-Änderungszähler den Grenzwert innerhalb einer bestimmten Dauer überschreitet, sendet er ein Trap an WCS. Das Trap enthält die Anzahl der MAP-Änderungen und die Dauer der Zeit. Wenn es z. B. innerhalb von 2 Minuten fünf Änderungen gibt, wird das Trap gesendet. Alarmschweregrad: Informatorisch.

- Child Excluded Parent (Übergeordneter untergeordneter untergeordneter Benutzer) - Dieser Alarm wird generiert, wenn ein übergeordnetes Element auf Blacklists gesetzt ist. Ein untergeordnetes Element kann ein übergeordnetes Element Blacklist erstellen, wenn das untergeordnete Element nach einer bestimmten Anzahl von Versuchen nicht authentifiziert werden konnte. Das Kind erinnert sich an die übergeordnete Blacklist, und wenn das Kind dem Netzwerk beitritt, sendet es das Trap, das die übergeordnete Blacklist-Adresse und die Dauer des Blacklist-Zeitraums enthält.

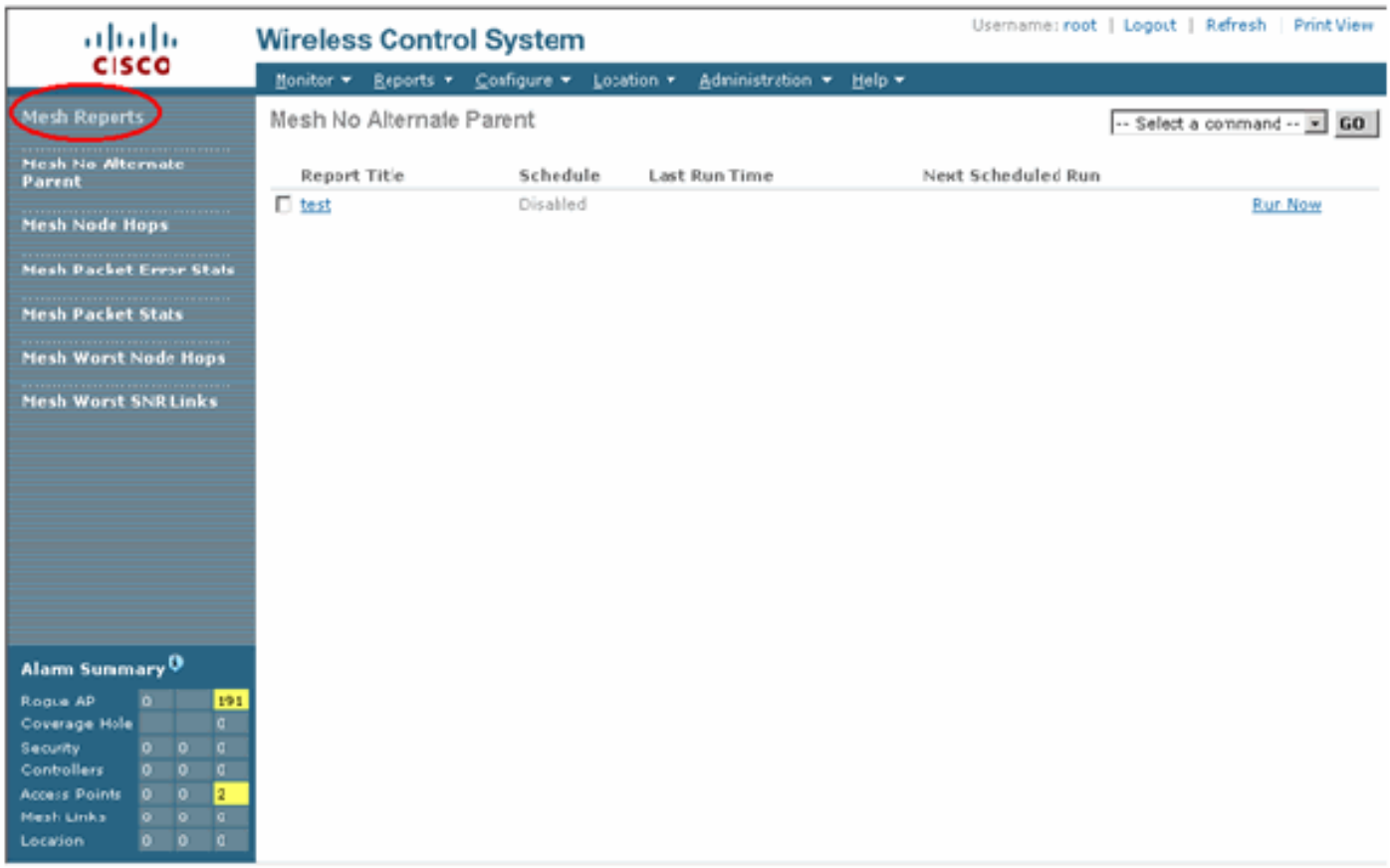
Alarme außer Indoor-Mesh-Links:

- Konsolenport-Zugriff - Der Konsolenport bietet dem Kunden die Möglichkeit, den Benutzernamen und das Kennwort zu ändern, um den gestrandeten Access Point für den Außenbereich wiederherzustellen. Um jedoch einen autorisierten Benutzerzugriff auf den Access Point zu verhindern, muss WCS einen Alarm senden, wenn jemand versucht, sich anzumelden. Dieser Alarm ist erforderlich, um Schutz zu bieten, da der Access Point im Freien physisch verwundbar ist. Dieser Alarm wird generiert, wenn sich der Benutzer erfolgreich am Konsolenport des AP angemeldet hat oder wenn er dreimal hintereinander versagt hat.
- MAC Authorization Failure (MAC-Autorisierungsfehler) - Dieser Alarm wird generiert, wenn der Access Point versucht, dem Indoor Mesh beizutreten, sich aber nicht authentifizieren kann, weil er nicht in der MAC-Filterliste enthalten ist. WCS empfängt ein Trap vom Controller. Das Trap enthält die MAC-Adresse des Access Points, bei dem die Autorisierung fehlgeschlagen ist.

Mesh-Bericht und Statistiken

Wir übernehmen den erweiterten Bericht- und Statistikrahmen ab 4.1.185.0:

- Kein Alternativer Pfad
- Mesh-Knoten-Hops
- Paketfehlerstatistiken
- Paketstatus
- Knoten-Hop mit schlechtem Ergebnis
- Schlimmste SNR-Links



Kein Alternativer Pfad

Indoor Mesh AP hat in der Regel mehr als einen Nachbarn. Falls ein inländischer Mesh-Access Point seine übergeordnete Verbindung verlässt, sollte der Access Point in der Lage sein, den alternativen übergeordneten Access Point zu finden. In manchen Fällen, wenn keine Nachbarn gezeigt werden, kann der Access Point keine anderen Eltern besuchen, wenn er seine Eltern verliert. Der Benutzer muss wissen, welche APs keine alternativen Eltern haben. Dieser Bericht listet alle APs auf, die keine anderen Nachbarn als die aktuellen übergeordneten Access Points haben.

Mesh-Knoten-Hops

Dieser Bericht zeigt die Anzahl der Hops außerhalb des Root AP (RAP). Sie können den Bericht anhand der folgenden Kriterien erstellen:

- AP über Controller
- Access Point auf Stockwerk

Paketfehlerraten

Die Paketfehler können durch Interferenzen und Paketverluste verursacht werden. Die Berechnung der Paketfehlerrate basiert auf gesendeten und erfolgreich gesendeten Paketen. Die Paketfehlerrate wird auf der Backhaul-Verbindung gemessen und sowohl für Nachbarn als auch für die übergeordneten Elemente erfasst. Der AP sendet regelmäßig Paketinformationen an den Controller. Sobald sich die übergeordnete Instanz ändert, sendet der Access Point die gesammelten Paketfehlerinformationen an den Controller. WCS fragt standardmäßig alle 10 Minuten Paketfehlerinformationen vom Controller ab und speichert diese in der Datenbank für bis zu 7 Tage. In WCS wird die Paketfehlerrate als Diagramm angezeigt. Das Paketfehlerdiagramm

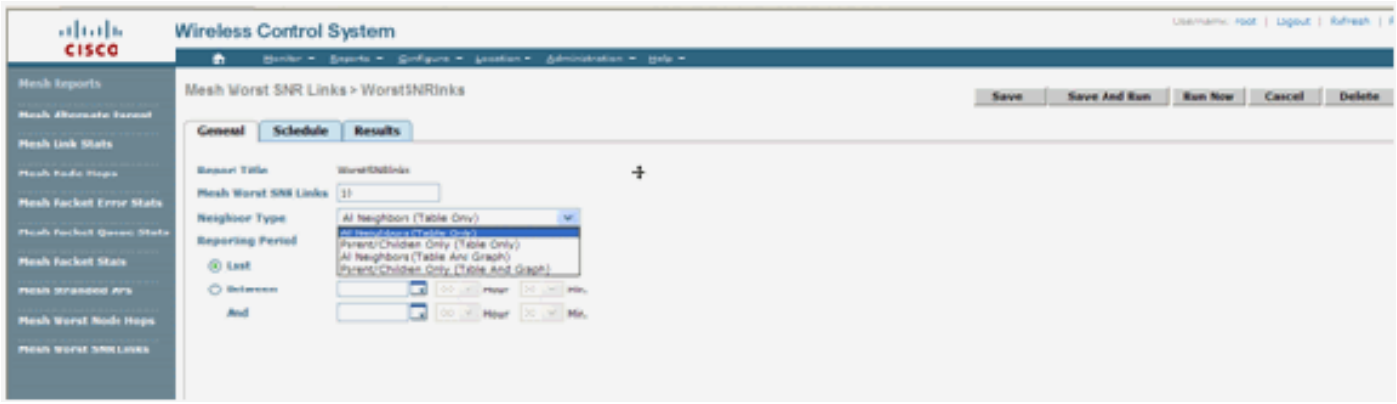
basiert auf den in der Datenbank gespeicherten Verlaufsdaten.

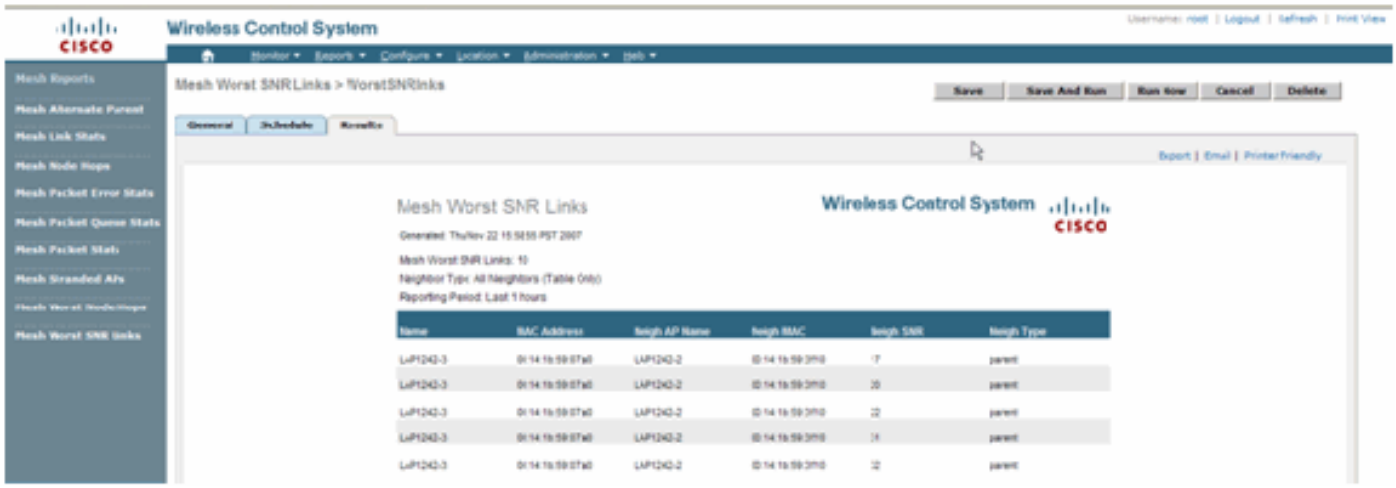
Paketstatus

Dieser Bericht zeigt die Zählerwerte der Gesamtzahl der Pakete, die von Nachbarn übertragen werden, und der Gesamtzahl der Pakete, die erfolgreich übertragen wurden. Sie können den Bericht anhand bestimmter Kriterien erstellen.

Die schlechtesten SNR-Verbindungen

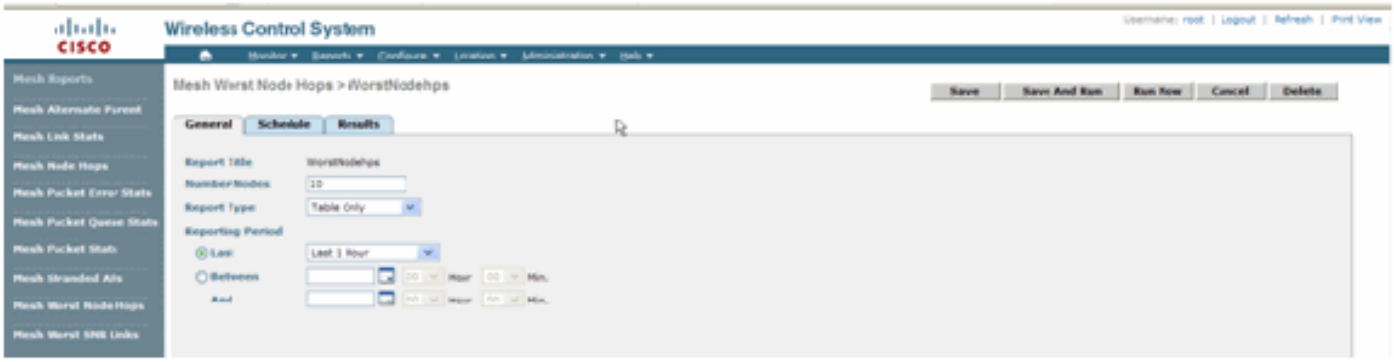
Geräuschprobleme können zu unterschiedlichen Zeiten auftreten, und die Geräusche können sich in unterschiedlichen Abständen oder über unterschiedliche Zeiträume vergrößern. Die nächste Abbildung bietet die Möglichkeit, Berichte für Radio a und b/g sowie für selektive Schnittstellen zu erstellen. Im Bericht werden standardmäßig die 10 schlechtesten SNR-Links aufgeführt. Sie können zwischen 5 und 50 schlechtesten Links wählen. Der Bericht kann für die letzten 1 Stunde, die letzten 6 Stunden, den letzten Tag, die letzten 2 Tage und bis zu 7 Tage erstellt werden. Die Daten werden standardmäßig alle 10 Minuten abgefragt. Die Daten werden maximal sieben Tage lang in der Datenbank gespeichert. Die Auswahlkriterien für den Typ des Nachbarn können alle Nachbarn sein, nur Eltern/Kinder.



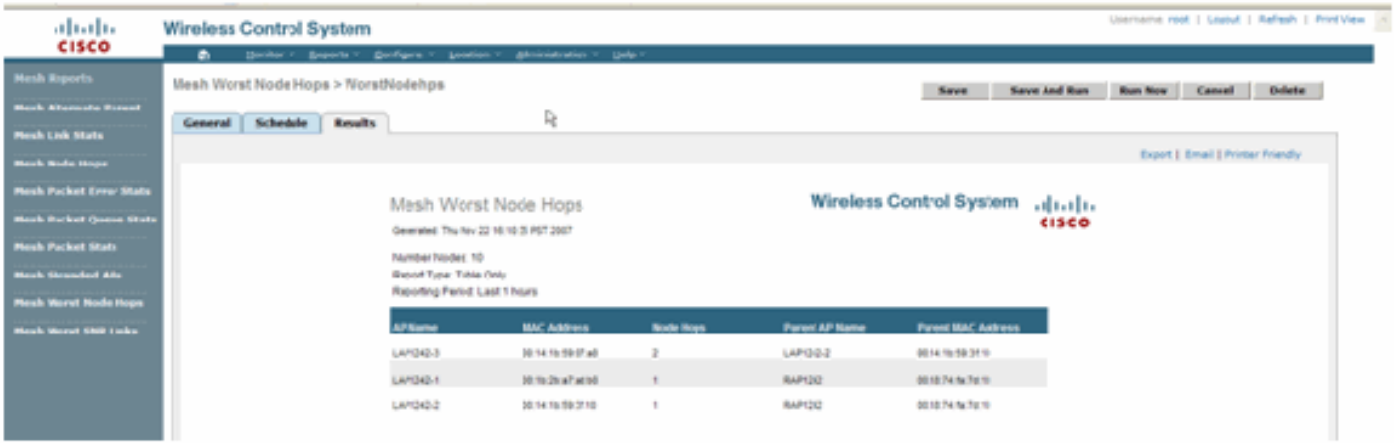


Hops mit schlechtem Knoten

Dieser Bericht listet standardmäßig die 10 schlechtesten Hops-APs auf. Wenn die APs zu viele Hops entfernt sind, können die Verbindungen sehr schwach sein. Der Benutzer kann die APs, die viele Hops von Root-APs entfernt haben, isolieren und entsprechende Maßnahmen ergreifen. Sie können die Kriterien **für die Anzahl der Knoten** zwischen 5 und 50 ändern. Die Filterkriterien für **Berichtstyp** in dieser Abbildung können nur Tabelle oder Tabelle und Diagramm sein:



Diese Abbildung zeigt das Ergebnis für den letzten Bericht:



Sicherheitsstatistiken

Die Statistiken zur Indoor Mesh Security werden auf der AP-Detailseite im Abschnitt Bridging Info (Bridging-Info) angezeigt. Ein Eintrag in der Indoor MeshNodeSecurity-Statistiktabelle wird erstellt, wenn ein untergeordneter Indoor-Mesh-Knoten einem übergeordneten Indoor-Mesh-Knoten zugeordnet wird oder sich bei diesem authentifiziert. Einträge werden entfernt, wenn der Indoor Mesh-Knoten vom Controller getrennt wird.

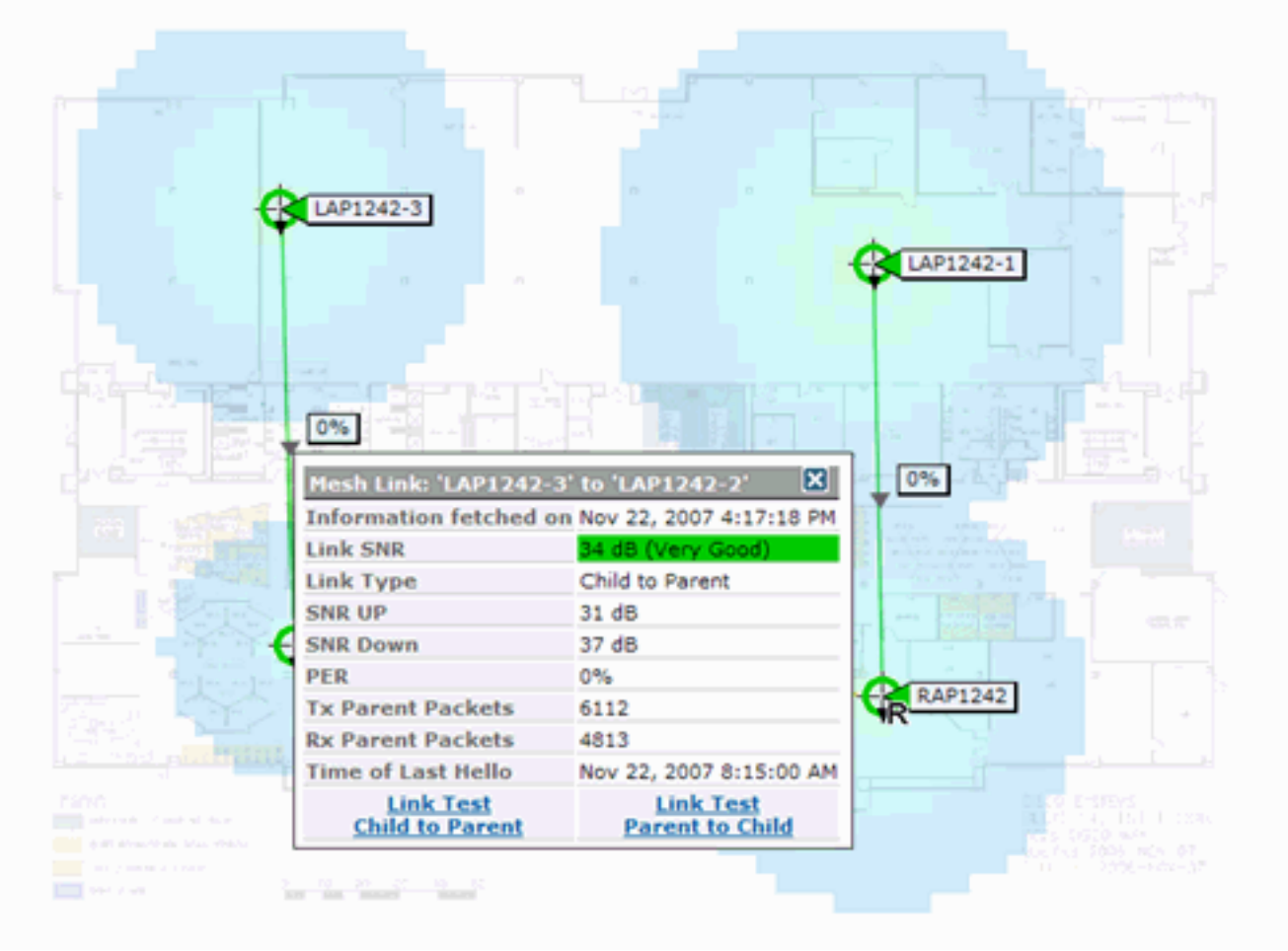
Verbindungstest

Der Verbindungstest zwischen AP und AP wird vom WCS unterstützt. Man kann zwei beliebige APs auswählen und einen Verbindungstest zwischen diesen beiden durchführen.

Wenn es sich bei diesen APs um RF-Nachbarn handelt, kann der Verbindungstest zu Ergebnissen führen. Das Ergebnis wird in einem Dialog auf der Karte angezeigt, ohne dass eine komplette Aktualisierung der Seite notwendig ist. Der Dialog kann leicht entsorgt werden.

Wenn diese beiden APs jedoch keine RF-Nachbarn sind, versucht WCS nicht, einen Pfad zwischen den beiden APs zu ermitteln, um einen kombinierten Verbindungstest durchzuführen.

Wenn die Maus über den Pfeil zwischen den beiden Knoten bewegt wird, wird dieses Fenster angezeigt:



Node-to-Node-Verbindungstest

Das Verbindungstest-Tool ist ein bedarfsorientiertes Tool zur Überprüfung der Verbindungsqualität zwischen zwei APs. In WCS wird diese Funktion auf der AP-Detailseite hinzugefügt.

Auf der Seite "AP detail" unter der Registerkarte **Indoor Mesh Link**, neben der Links aufgeführt sind, gibt es einen Link zum Durchführen des Verbindungstests.

Das CLI Link Test-Tool des Controllers verfügt über die optionalen Eingabeparameter: Paketgröße, Gesamtverbindungstestpakete, Testdauer und Datenübertragungsrate. Der Verbindungstest enthält Standardwerte für diese optionalen Parameter. Die MAC-Adressen für die Knoten sind die einzigen obligatorischen Eingabeparameter.

Das Link Test-Tool testet die Stärke, das gesendete Paket und das zwischen den Knoten empfangene Paket. Der Link für Verbindungstest wird im AP-Detailbericht angezeigt. Wenn Sie auf den Link klicken, wird ein Popup-Bildschirm mit den Ergebnissen des Verbindungstests angezeigt. Der Verbindungstest gilt nur für Parent-Child und für Nachbarn.

Die Ausgabe des Verbindungstests generiert gesendete Pakete, empfangene Pakete, Fehlerpakete (aus unterschiedlichen Gründen in Eckets), SNR, Noise Floor und RSSI.

Der Linktest bietet mindestens folgende Details über die Benutzeroberfläche:

- Gesendete Verbindungstest-Pakete
- Empfangene Verbindungstest-Pakete
- Signalstärke in dBm

- Signal-Rausch-Verhältnis

On-Demand-AP-Nachbarverbindungen

Dies ist eine neue Funktion in der WCS Map. Sie können auf einen Mesh-Access Point klicken und ein Popup-Fenster mit Detailinformationen wird angezeigt. Sie können dann auf **Mesh Neighbors anzeigen** klicken, um die Nachbarinformationen für den ausgewählten Access Point abzurufen und eine Tabelle mit allen Nachbarn für den ausgewählten Mesh-Access Point für Innenbereiche anzuzeigen.

Der View Mesh Neighbor Link zeigt alle Nachbarn für den markierten Access Point an. Dieser Snapshot zeigt alle Nachbarn, den Typ der Nachbarn und den SNR-Wert.

Ping-Test

Der Ping-Test ist ein On-Demand-Tool, mit dem Pings zwischen dem Controller und dem AP durchgeführt werden. Das Ping Test Tool ist sowohl auf der AP-Detailseite als auch auf der MAP-Seite verfügbar. Klicken Sie auf den Link **Ping-Test ausführen** entweder auf der AP-Detailseite oder auf der MAP-AP-Info, um den Ping vom Controller zum aktuellen Access Point zu initiieren.

Fazit

Enterprise Mesh (d. h. ein Indoor-Mesh) ist eine Erweiterung der Cisco Wireless-Abdeckung für Orte, an denen kabelgebundenes Ethernet keine Konnektivität bereitstellen kann. Die Flexibilität und Verwaltbarkeit eines Wireless-Netzwerks wird durch Enterprise Mesh erreicht.

Die meisten Funktionen, die kabelgebundene APs bieten, werden durch die Indoor-Mesh-Topologie bereitgestellt. Ein Enterprise Mesh-Netzwerk kann auch zusammen mit den kabelgebundenen APs auf demselben Controller vorhanden sein.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme