Bereitstellungsleitfaden für Cisco Wireless Controller der Serie 8500

Inhalt

Einführung

In diesem Dokument wird der Cisco 8500 Wireless LAN Controller (WLC) vorgestellt und es werden allgemeine Richtlinien für seine Bereitstellung bereitgestellt. Ziel dieses Dokuments ist es,

- Bieten Sie einen Überblick über den Cisco 8500 WLC und seine Bereitstellung innerhalb der Cisco Unified Architecture.
- Wichtigste Service Provider-Funktionen hervorheben
- Stellen Sie spezifische Designempfehlungen und -überlegungen für den Cisco 8500 Controller bereit.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

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

Konventionen

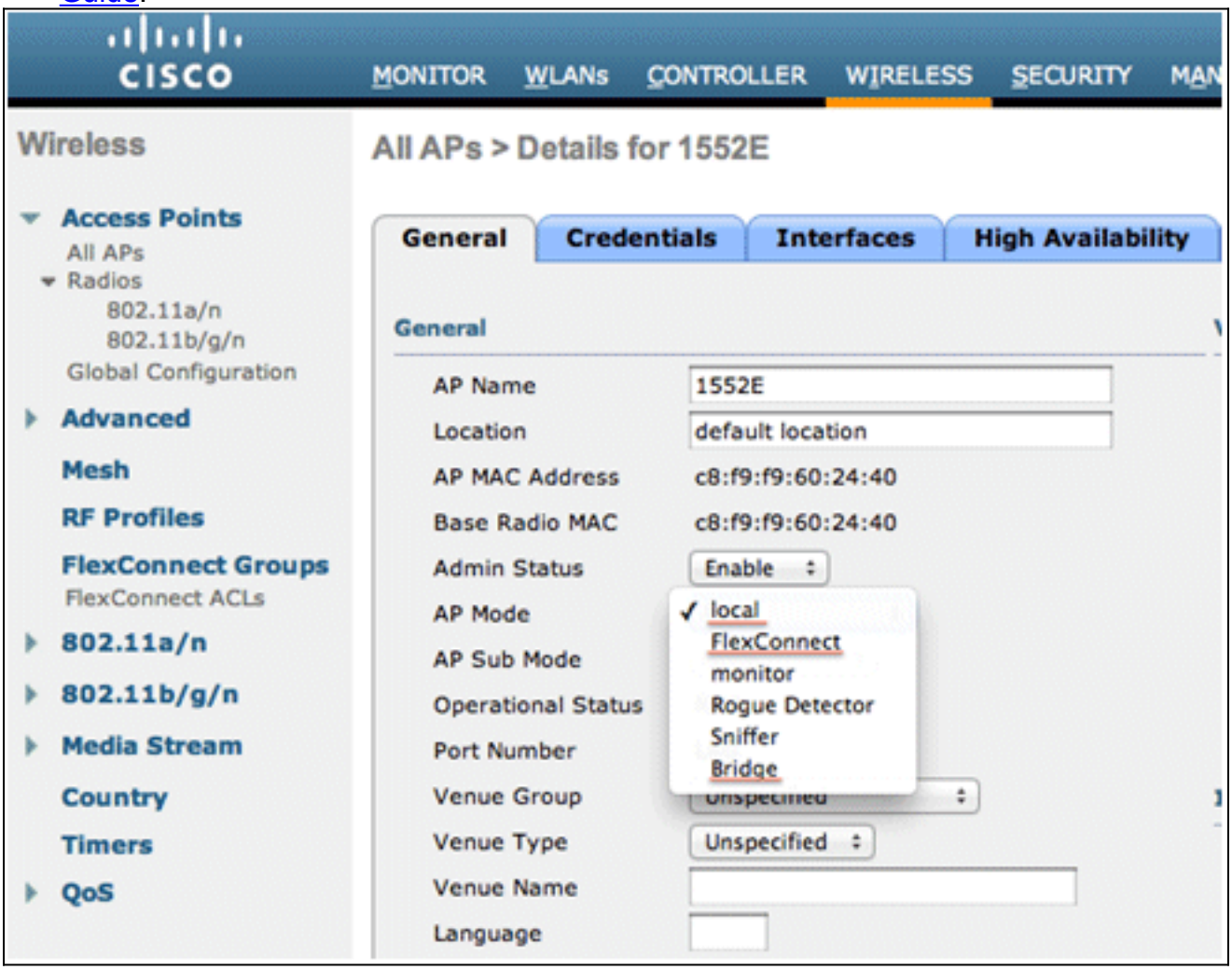
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Produktübersicht

In der Cisco Unified Architecture wird ein Wireless Access Point (AP) in einem von drei Hauptmodi bereitgestellt, um Wireless-Clients zu bedienen:

- **Lokaler Modus** - Ein AP im lokalen Modus leitet den gesamten Datenverkehr (über CAPWAP) an den Controller weiter, wo der Controller das Tagging der Pakete übernimmt und sie im kabelgebundenen Netzwerk ablegt.
- **FlexConnect-Modus** - Der FlexConnect-Modus ist in erster Linie für die Unterstützung von Wireless-Zweigstellennetzwerken konzipiert, da die Daten lokal geswitcht werden können (mit Unterstützung für zentrales Switching am Controller), während die APs über eine WAN-Verbindung über einen zentralen Controller gesteuert und verwaltet werden. Der Datenverkehrsfluss von einem FlexConnect-AP kann den effizientesten Pfad verwenden, da der Administrator die Flexibilität hat, bestimmte Arten von Datenverkehr für das lokale Switching zu konfigurieren, oder ihn für das zentrale Switching am Controller in der Zentrale tunneln lassen kann. Weitere Informationen zur FlexConnect-Betriebstheorie finden Sie im H-Reap/FlexConnect-Designleitfaden und im Cisco Flex 7500-Bereitstellungsleitfaden.

- **Bridge-Modus** - Ein Access Point im Bridge-Modus ist für den Aufbau eines drahtlosen Mesh-Netzwerks konfiguriert, in dem keine kabelgebundene Netzwerkverkabelung verfügbar ist. Weitere Informationen zur Mesh-Betriebstheorie finden Sie im Mesh Design and Deployment Guide.



Sowohl der Cisco Controller der Serie 5500 als auch der WiSM2-Controller unterstützen alle AP-Betriebsmodi, die auf bis zu 500 bzw. 1.000 APs bzw. 7.000 bzw. 15.000 Wireless-Clients skaliert werden können. Die explosionsartige Verbreitung mobiler Clients im Unternehmen, die durch BYOD (Bring Your Own Device), die Bereitstellung von Wireless-Netzwerken in geschäftskritischen Anwendungen und die Einführung von Wi-Fi in Service Provider-Netzwerken, die neue Geschäftsmodelle ermöglichen, erfordern drahtlose Netzwerke, um eine höhere Client-Skalierbarkeit, eine höhere Ausfallsicherheit und eine nahtlose IP-Mobilität zwischen Mobilfunk- und Wi-Fi-Netzwerken bereitzustellen. Die Cisco Unified Wireless Network Software Version 7.3 adressiert diese wichtigen Herausforderungen. Version 7.3 bietet den neuen Cisco Wireless Controller der Serie 8500 mit einer hochgradig skalierbaren Client-Anzahl, einer Hochverfügbarkeitsfunktion, die die Ausfallzeiten von Controllern minimiert, indem Tausende von Access Points in einem Standby-Controller in Sekundenbruchteilen gesichert werden können, und Service Provider-Funktionen wie Wi-Fi Certified Passpoint (HS2.0) für eine sichere öffentliche Anbindung und Proxy Mobile IPv6 (PMIPv6). Mobilität zwischen Mobilfunk und Wi-Fi.

Einige der wichtigsten Merkmale des Cisco 8500 Controllers sind:

- Hohe Client-Dichte (64.000 Clients in einer HE)
- Unterstützung für 6.000 APs, 6.000 AP-Gruppen, 2.000 FlexConnect-Gruppen und bis zu 100 APs pro FlexConnect-Gruppe

- Unterstützung für 4096 VLANs
- Unterstützung für 50.000 RFID-Nachverfolgung sowie Erkennung und Eindämmung von bis zu 24.000 nicht autorisierten APs und bis zu 32.000 nicht autorisierten Clients
- HA mit Stateful Switchover für AP im Bruchteil einer Sekunde
- Unterstützung für APs im Außenbereich
- Unterstützung aller AP-Betriebsmodi (lokal, FlexConnect, Monitor, Rogue Detector, Sniffer und Bridge)
- Nahtlose Mobilität mit dem Packet Core-Netzwerk mit PMIPv6 MAG-Implementierung (RFC 5213)
- WFA Passpoint-Zertifizierung (in Bearbeitung - WFA-Website auf aktuellsten Status überprüfen)
- 802.11r Fast Roaming
- Bidirektionale Durchsatzbegrenzung für Datenverkehrsflüsse
- Video-Stream für Rich Media-Datenströme
- Nutzungsrechte (RTU)-Lizenzierung zur Vereinfachung der Lizenzaktivierung und laufender Lizenzierungsvorgänge

Diese Tabelle zeigt den Vergleich von Cisco High-Scale-Controllern auf einen Blick:

	8500	7500	5500	WiSM2
Bereitstellungsart	Großunternehmen Campus + SP Wi-Fi	Zentraler Standort-Controller für eine große Anzahl verteilter, Controller-loser Zweigstellen	Enterprise Campus und Filiale mit vollständigem Service	Enterprise-Campus
Betriebsmodi	Lokaler Modus, FlexConnect, Mesh	Nur FlexConnect	Lokaler Modus, FlexConnect, Mesh	Lokaler Modus, FlexConnect, Mesh
Maximale Skalierung	6.000 APs 64.000 Clients	6.000 APs 64.000 Clients	500 APs 7.000 Clients	1.000 APs 15.000 Clients
AP-Zählbereich	300-6.000 APs	300-6.000 APs	12-500 APs	100-1.000 APs
Lizenzierung	Nutzungsrecht (mit EULA)	Nutzungsrecht (mit EULA)	CISL-basiert (unverändert)	CISL-basiert (unverändert)
Konnektivit	2 x 10-G-	2 x 10-G-	8 x	Interne

ät	Ports	Ports	1G-Ports	Verbindungen zu den Catalyst Backplanes
Stromversorgung	Wechselstrom/Gleichstrom, dual-redundant	Wechselstrom, dual, redundant	Wechselstrom (redundante PSU-Option)	Redundante PSU-Option für AC/DC Catalyst-Chassis
Maximale Anzahl an FlexConnect-Gruppen	2000	2000	100	100
Maximale Anzahl von APs pro FlexConnect-Gruppe	100	100	25	25
Maximale Anzahl Management von nicht autorisierten Access Points	24.000	24.000	2000	4000
Maximale Anzahl Management von nicht autorisierten Clients	32.000	32.000	2500	5000
Maximale Anzahl an RFID	50.000	50.000	5000	10.000
Maximale APs pro RRM-Gruppe	6000	6000	1000	2000
Maximale AP-Gruppen	6000	6000	500	500
Maximale Schnittstellengruppen	512	512	64	64

Maximale Schnittstellen pro Schnittstellengruppe	64	64	64	64
Maximale Anzahl unterstützter VLANs	4096	4096	512	512
Maximale Anzahl unterstützter WLANs	512	512	512	512
Unterstützte Fast Secure Roaming (FSR)-Clients*	64000	64000	14.000	30.000

***** Unterstützte Anzahl von FSR-Clients für diese Plattform (weitere Einzelheiten finden Sie im Abschnitt Überlegungen zum Design unter Plattformübergreifende Mobilität).

Produktspezifikationen

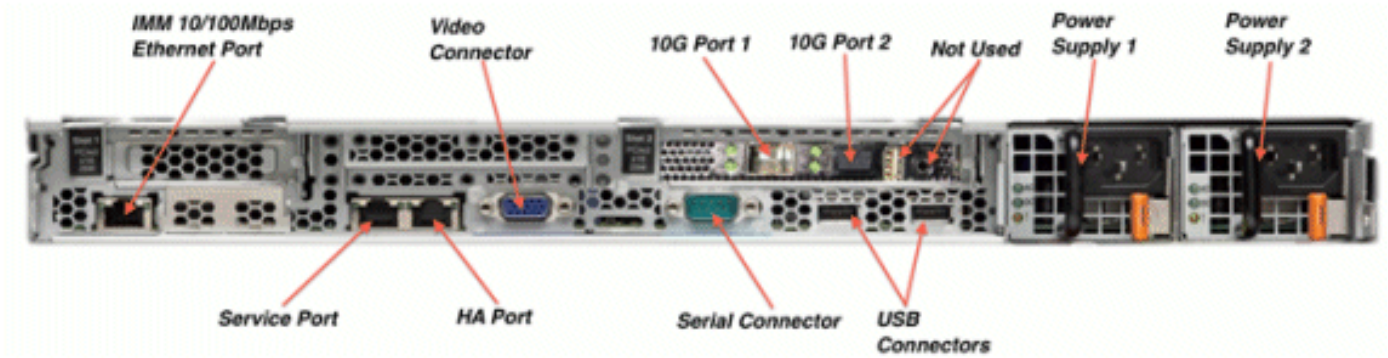
Datenblatt

Weitere Informationen finden Sie im Datenblatt zu Cisco Controllern der Serie 8500.

Plattformfunktionen

Front view:

Rear View:



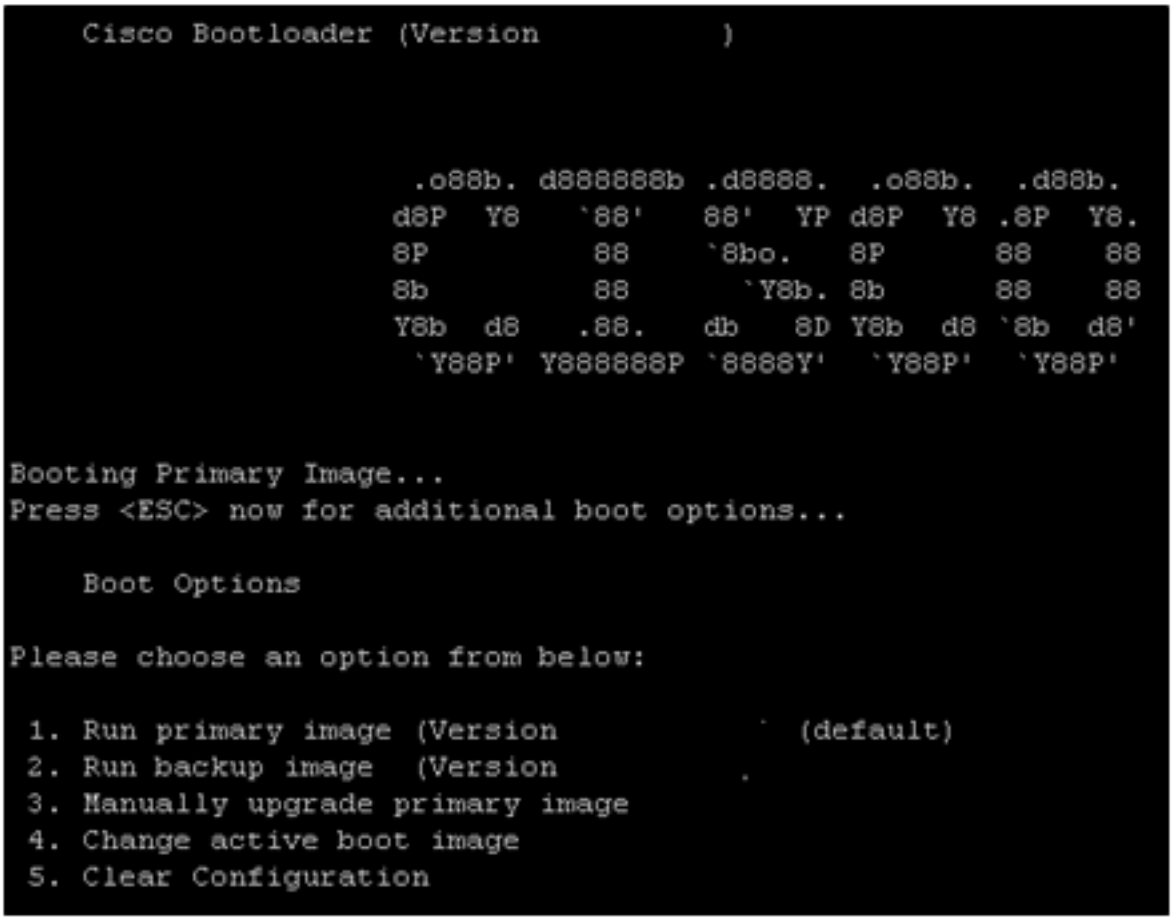
Funktionen, die derzeit nicht von der 8500-Controller-Plattform unterstützt werden

Diese Funktionen werden derzeit auf der 8500 Controller-Plattform nicht unterstützt:

- Lokale Authentifizierung (wobei der Controller als Authentifizierungsserver fungiert)
- Interner DHCP-Server
- Kabelgebundener Gast
- TrustSec SXP

Look and Feel des Cisco 8500 Controllers

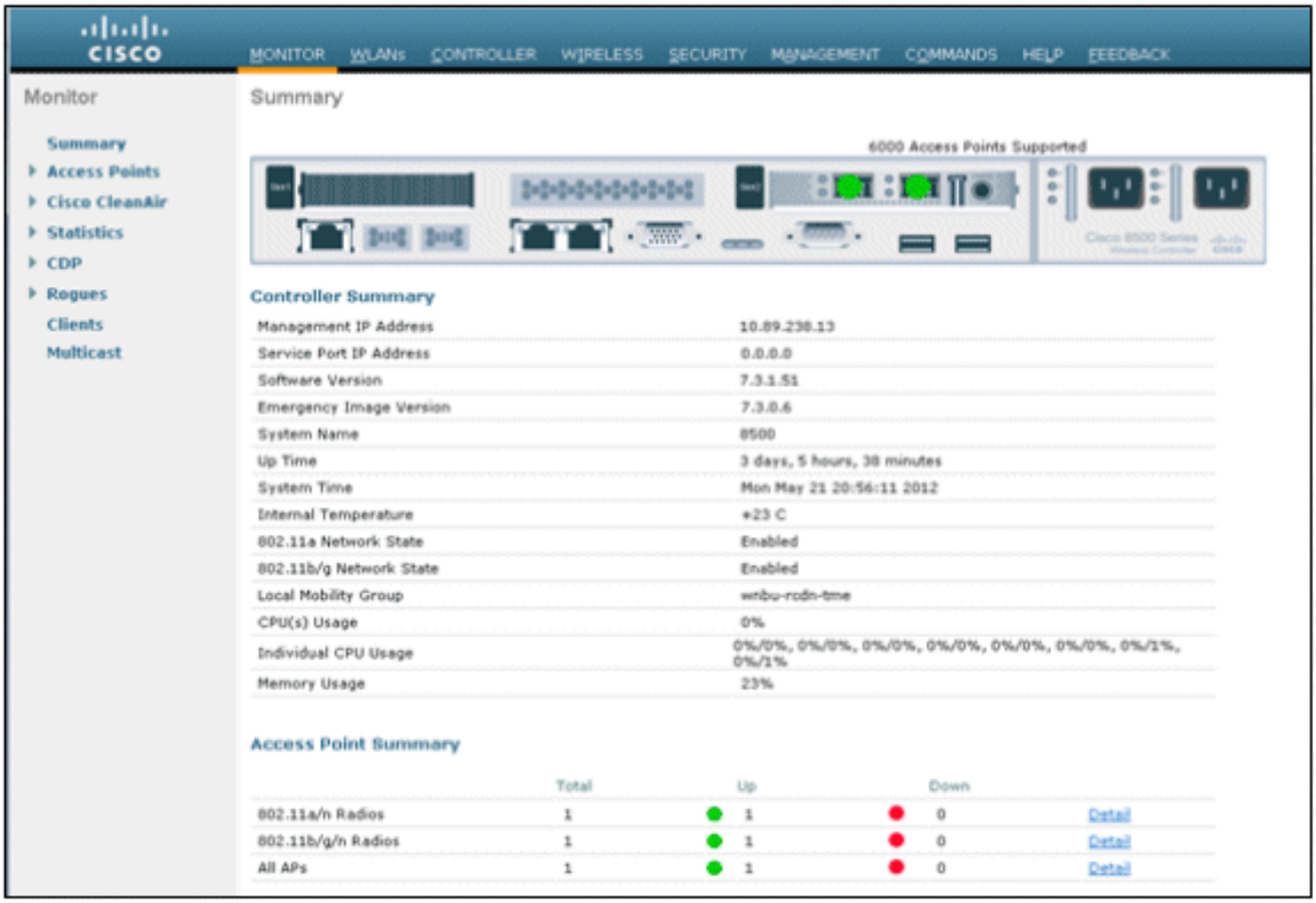
Der Cisco 8500 Controller aktiviert standardmäßig die Konsolenumleitung, wobei die Baudrate 9600 ein VT100-Terminal ohne Flusssteuerung simuliert. Der Controller 8500 verfügt über die gleiche Bootreihenfolge wie die vorhandenen Controller-Plattformen.



Wie bei allen anderen Controller-Plattformen muss für das erstmalige Booten die Konfiguration über das Menü "Assistent" erfolgen.

```
Would you like to terminate autoinstall? [yes]:

System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *******
Re-enter Administrative Password                  : *******

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: Yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```


Die Benutzeroberfläche bleibt auch mit den vorherigen Controllern identisch.



Hervorhebung der Funktionen im Cisco Controller der Serie 8500

Skalierbarkeit

Der Cisco WLC der Serie 8500 bietet Skalierbarkeit der Service Provider-Klasse in einem kleinen 1-HE-Formfaktor. Service Provider können mehrere Controller konsolidieren und die Betriebskosten durch einen zentralen Verwaltungs- und Kontrollpunkt für bis zu 64.000 Clients senken, die auf 4.096 VLANs und 6.000 APs verteilt sind.

Unterstützung des lokalen Modus

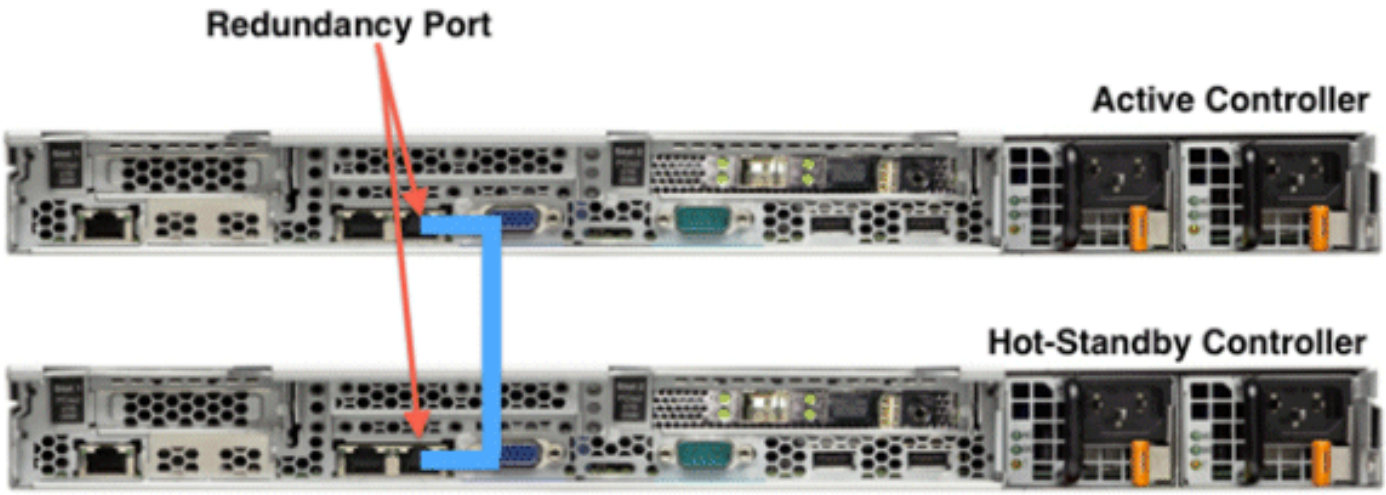
Die Cisco 8500 Controller-Plattform unterstützt APs im lokalen Modus, Bridge-Modus und FlexConnect-Modus. Der Controller 8500 unterstützt alle AP-Modelle, die von einem Cisco Controller der Serie 5500 mit Softwareversion 7.3 unterstützt werden.

Hohe Verfügbarkeit - AP Stateful Switchover

Im herkömmlichen Controller-AP-Fail-Over-Modell wurde für jeden Access Point eine eindeutige IP-Adresse für den primären, sekundären und dritten Controller konfiguriert. Wenn der aktive Controller des Access Points ausfiel, wechselte der Access Point in den Erkennungsstatus, und es war ein vollständiger Vorgang zum Beitritt zu einem neuen Controller erforderlich.

Das neu eingeführte Stateful Switchover (AP SSO)-Modell mit hoher Verfügbarkeit bietet eine Box-to-Box-Redundanz mit einem Controller im aktiven Zustand und einem zweiten Controller im Hot Standby-Zustand, bei dem der Status des aktiven Controllers über einen redundanten (HA)-

Port überwacht wird.



Die Konfiguration auf dem aktiven Controller wird über den redundanten Port mit dem Standby-Controller synchronisiert. In HA verwenden beide Controller denselben Konfigurationssatz, einschließlich der IP-Adresse der Verwaltungsschnittstelle. Darüber hinaus werden auch der CAPWAP-Status des Access Points (für APs im RUN-Status) synchronisiert. So wechseln APs nicht in den Discovery-Status, wenn der aktive Controller ausfällt. Dieses Modell reduziert die Ausfallzeiten bei einem Box-Ausfall auf Sekundenbruchteile und bei Upstream-Netzwerkverbindungsproblemen (z. B. Gateway-Verlust) auf bis zu drei Sekunden.

Hinweis: Die HA/AP-SSO-Funktion wird auch auf den Plattformen 5500, 7500 und WiSM-2 unterstützt, auf denen der 7.3-Versionscode ausgeführt wird.

Eine dedizierte Standby-Controller-SKU (AIR-CT8510-HA-K9) ist verfügbar und unterstützt den Standby-Betrieb für bis zu 6.000 APs, wenn sie, wie hier beschrieben, mit dem primären 8500-Controller verbunden wird.

Weitere Informationen zur HA-Funktion finden Sie im Bereitstellungsleitfaden für die Hochverfügbarkeit (AP SSO).

Neues Lizenzierungsmodell

Version 7.3 führt außerdem ein neues RTU-Lizenzmodell (Right to Use) für die Cisco Flex-Controller der Serien 7500 und 8500 ein. Dieses Honorar-basierte Lizenzierungsschema ermöglicht die Aktivierung von AP-Lizenzen auf unterstützten Controllern mit Endbenutzer-Lizenzvertrag (EULA)-Akzeptanz Das RTU-Lizenzschema vereinfacht das Hinzufügen, Löschen oder Übertragen von AP-Zusatzlizenzen vor Ort, da kein zusätzlicher Schritt, keine zusätzlichen Tools oder kein Zugriff auf Cisco.com für PAK-Lizenzen oder RMA-Übertragungen (Return Materials Authorization) erforderlich ist.

Evaluierungslizenzen sind 90 Tage gültig. Es werden Benachrichtigungen generiert, die Sie darüber informieren, dass Sie eine permanente Lizenz ab 15 Tagen vor Ablauf der Testlizenz erwerben.

Wenn mehr APs verbunden sind als gekaufte, wird der Lizenzierungsstatus für den in der Cisco Prime-Infrastruktur 1.2 verfolgten Controller rot.

Weitere Informationen zum RTU-Lizenzmodell finden Sie im Dokument Cisco Right to Use

Licensing (RTU).

Lizenztypen

Es gibt drei Lizenztypen:

- **Permanente Lizenzen** - Die AP-Anzahl wird von der Fertigung in NVM programmiert. Dies wird auch als Base AP Count Licenses bezeichnet. Diese Lizenzart ist nicht übertragbar.
- **Zusatzlizenzen für die Anzahl der Access Points** - Sie können durch die Annahme des EULA aktiviert werden. Zusatzlizenzen sind übertragbar.
- **Evaluierungslizenzen** - Diese Lizenzen werden für Demo- und/oder Testzeiträume verwendet. Sie sind 90 Tage gültig und werden standardmäßig mit der vollen Kapazität des Controllers ausgeschöpft. Die Evaluierungslizenz kann jederzeit mit einem CLI-Befehl aktiviert werden.

CLI-Befehle für Lizenzen:

```
(8500) >show license ?

all             Displays All The License(s).
capacity        Displays License currently used by AP
detail          Displays Details Of A Given License.
evaluation      Displays Evaluation License(s).
expiring        Displays Expiring License(s).
feature         Displays License Enabled Features.
in-use          Displays License That Are In-Use.
permanent       Displays Permanent License(s).
statistics      Displays License Statistics.
status          Displays License Status.
summary         Displays Brief Summary Of All License(s).
```

Nahtlose IP-Mobilität für die Paketkern-Integration mit dem WLC als PMIPv6 MAG

Proxy Mobile IPv6 (PMIPv6) ist ein netzwerkbasiertes IETF-Standard-Mobilitätsmanagement-Protokoll für den Aufbau gemeinsamer und zugangstechnologie-unabhängiger mobiler Kernnetzwerke (spezifiziert in RFC 5213). Es unterstützt verschiedene Zugriffstechnologien wie WiFi, WiMAX, 3GPP und 3GPP2-basierte Zugriffs-Architekturen. PMIPv6 bietet dieselbe Funktionalität wie Mobile IP, ohne dass Änderungen am TCP/IP-Protokoll-Stack des Hosts erforderlich sind. Mit PMIPv6 kann der Host seine Verbindungspunkte im Internet ändern, ohne seine IP-Adresse zu ändern. Diese Funktionalität wird vom Netzwerk implementiert, das für die Verfolgung der Bewegungen des Hosts und die Initiierung der erforderlichen Mobilitätssignalisierung in seinem Namen verantwortlich ist.

Die PMIPv6-Architektur definiert folgende funktionale Einheiten:

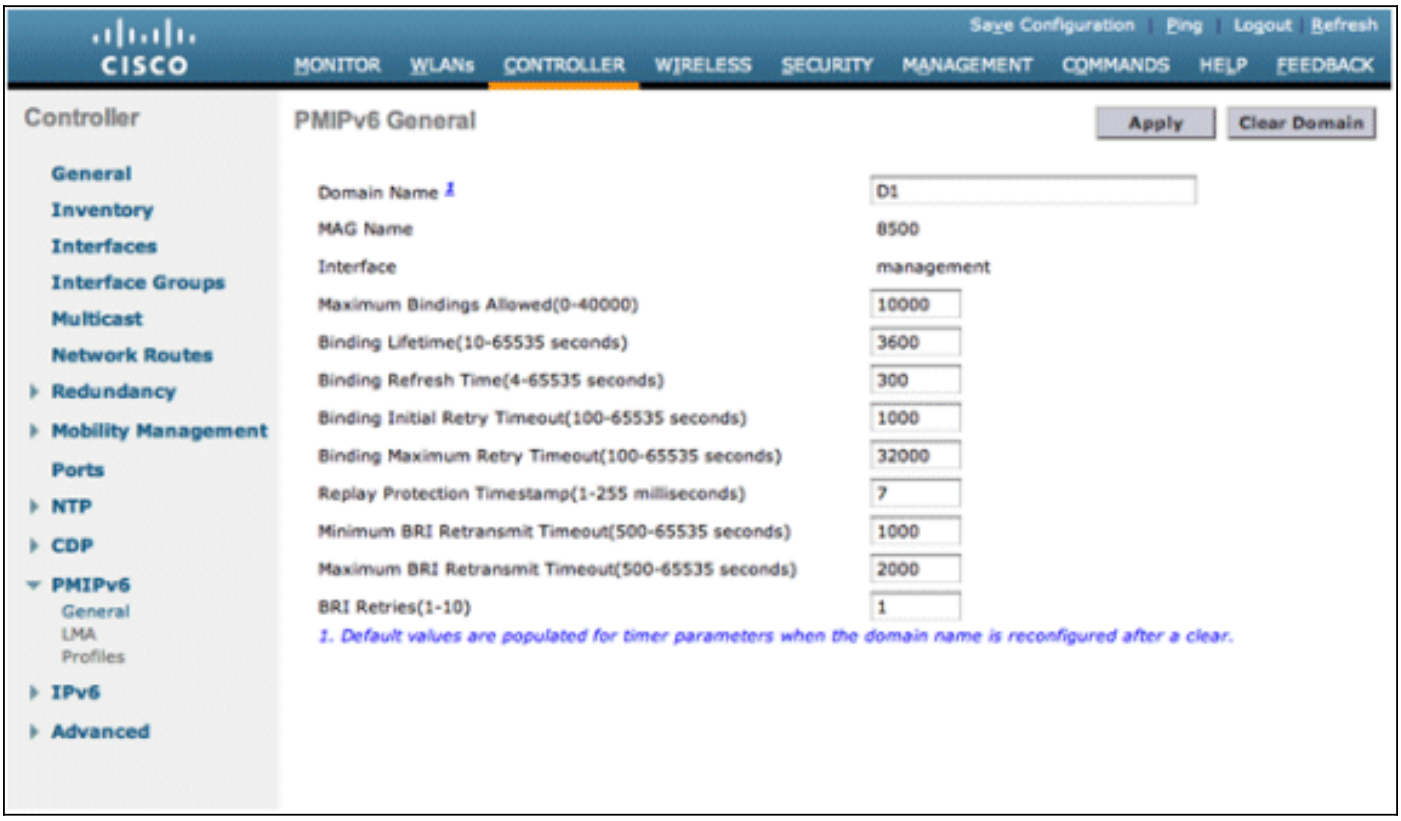
- Lokaler Mobility Anchor (LMA)
- Mobile Access Gateway (MAG)
- Mobiler Knoten (MN)
- Mobilfunknetze (CN)

Die LMA ist das zentrale Kernelement der PMIPv6-Architektur. Es ist der Punkt, an dem die MN-IP-Adressen zugewiesen und angezeigt werden. Die LMA stellt einen bidirektionalen Tunnel zum Controller her (mit Version 7.3 oder höher) und fungiert als PMIPv6 MAG. Die MAG (d. h. der Controller) interagiert mit der LMA und führt das Mobilitätsmanagement im Auftrag des Wireless-Clients (MN) durch.

Andere Geräte im Netzwerk (als CN definiert) können den Wireless-Client (MN) über seine Heimadresse über die LMA erreichen, die die Erreichbarkeit des MN-Präfix an die CN weitergibt.

Weitere Informationen zur PMIPv6-Funktion für nahtlose IP-Mobilität finden Sie im Konfigurationsleitfaden für Cisco Wireless Proxy Mobile IPv6.

Hier sehen Sie den allgemeinen Bildschirm für die PMIPv6-Einstellungen eines 8500-Controllers:



Hinweis: Die PMIPv6 MAG-Funktionalität ist derzeit nur für die Cisco Controller-Plattformen 8500, 5500 und WiSM-2 verfügbar.

Hinweis: Version 7.3 unterstützt die Kommunikation mit bis zu 10 LMAs und 40.000 PMIPv6-Clients.

WiFi Passpoint 1.0 (oder HotSpot 2.0)

Passpoint (HotSpot2.0) basiert auf drei technologischen Säulen: IEEE 802.11u-, WPA2-Enterprise- und EAP-basierte Authentifizierung

Wi-Fi-zertifizierter Passpoint (HS2.0) stellt eine einfache und sichere Verbindung zu öffentlichen Wi-Fi-Hotspots zum Auslagern von Mobilfunkdaten sicher und sorgt so für niedrigere Gesamtbetriebskosten.

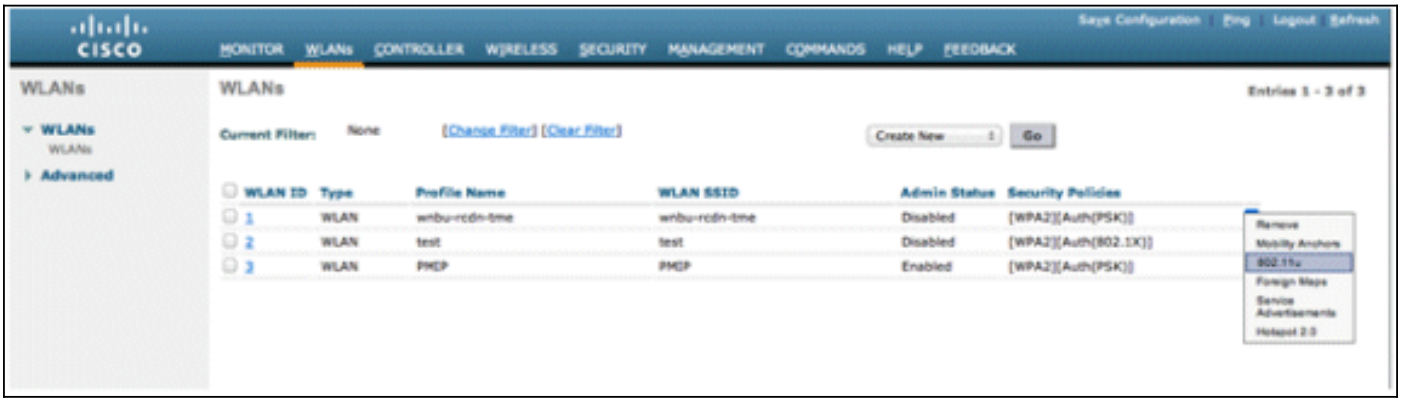
Die Unterstützung von HS2.0 ist für die folgenden AP-Betriebsarten verfügbar:

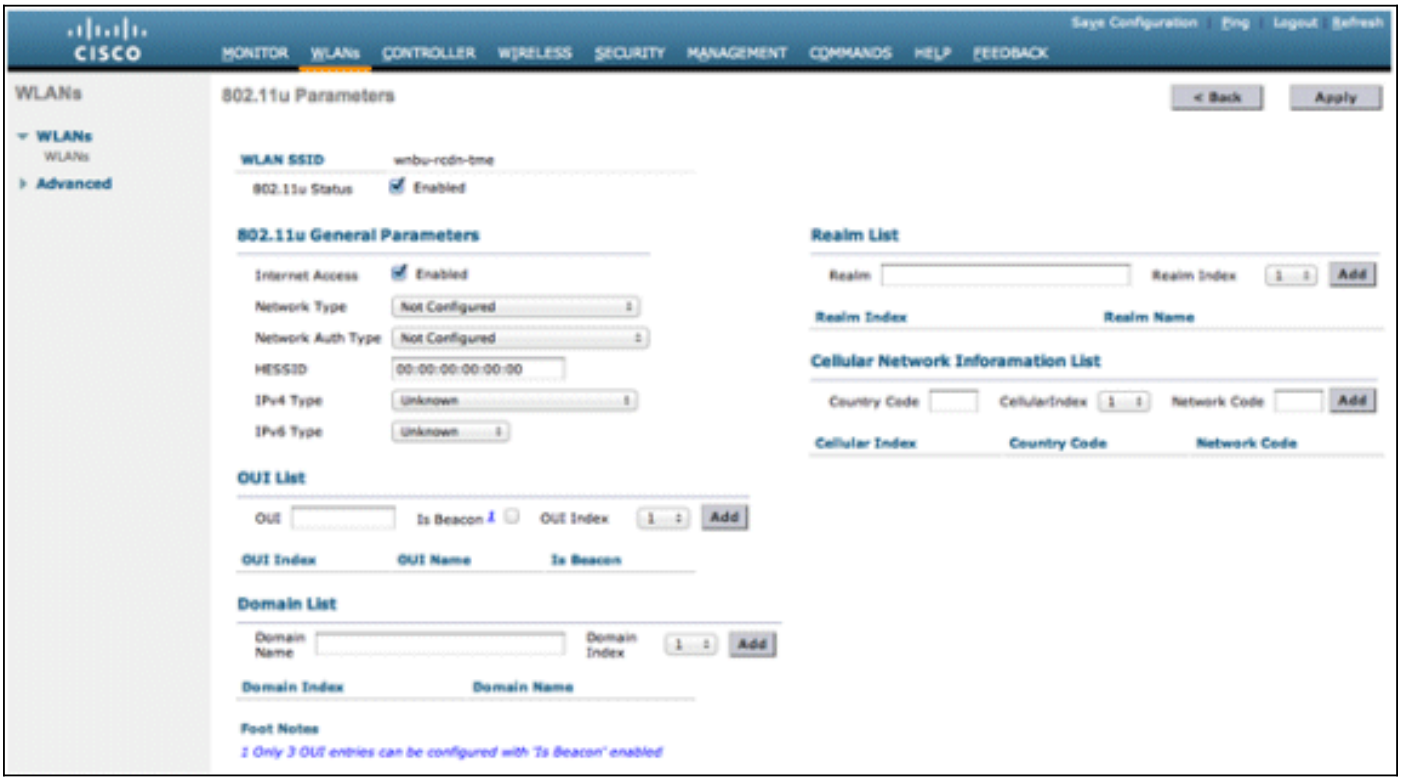
- AP im lokalen Modus
- AP im Bridge-Modus (nur Root-AP)
- FlexConnect sowohl Central Switch- als auch Local Switching-Modus

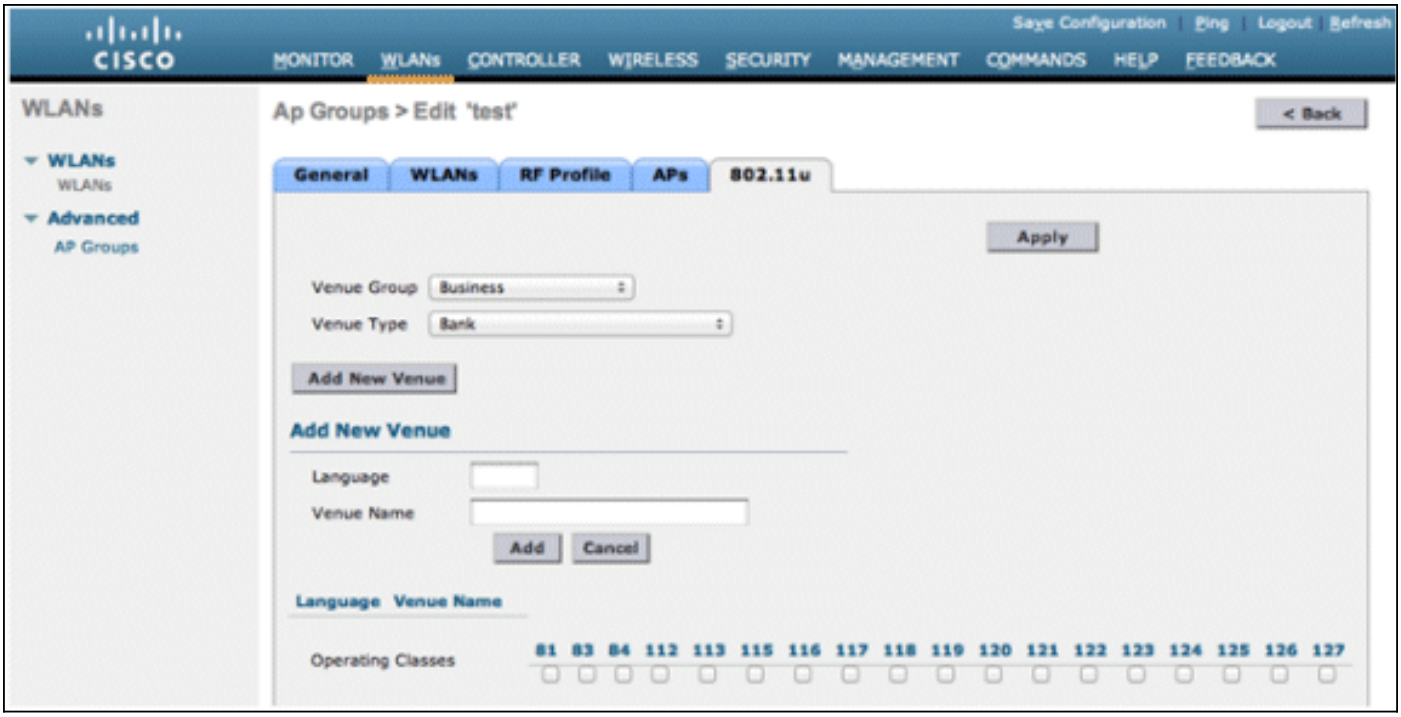
Hinweis: Die Passpoint-Funktionen sind in Softwareversion 7.3 für alle Controller-Plattformen und CAPWAPs verfügbar, die die Version 7.2 ausführen können (außer Office Extend AP600).

Weitere Informationen zum Konfigurieren dieser Funktionen finden Sie im Cisco Wireless LAN Controller Configuration Guide, Release 7.3.

Diese Bilder zeigen verschiedene 802.11u-Konfigurationsoptionen an:







4k VLAN-Unterstützung am Controller

Um die Skalierbarkeitsanforderungen des Service Providers zu erfüllen, erweitert die Softwareversion 7.3 die Anzahl der unterstützten VLANs auf 4.096.

Dies ermöglicht einen standortbasierten Service pro Schnittstelle/VLAN, da die Anzahl der maximal verfügbaren Schnittstellen von 512 auf 4096 (4095 + Management-Schnittstelle) und die zugehörigen VLANs erhöht wurde.

Hinweis: Das 4k VLAN wird nur von den Controllern 8500 und Flex7500 unterstützt.

Zweifach redundante Gleichstromversorgung

Um die Gleichstromanforderungen von Service Providern zu erfüllen, kann der 8500 in einer redundanten Konfiguration mit -48-V-Gleichstrom-Netzteil bestellt werden.

Eingangsspannungsbereich: Minimum: -40 V Gleichstrom und Maximum: -75 V Gleichstrom

Hinweis: Der 8510-Controller mit Gleichstrom wird nicht mit länderspezifischen Netzkabeln geliefert. Bei Gleichstromnetzteilen sollten Sie ein eigenes 12G-Kabel verwenden und eine Verbindung zum Gleichstromnetzteil herstellen.

Weitere wichtige, auf Service Provider ausgerichtete Funktionen

Die Cisco WLCs wurden mit dem 7.3-Code um weitere wichtige, auf Service Provider ausgerichtete Funktionen erweitert:

- Zentrales DHCP für lokales FlexConnect-Switching
- VLAN-Tagging für CAPWAP-Management (keine CAPWAP-Einschränkung für natives VLAN)
- Verbesserte RADIUS-Accounting-Funktionen
- Failover für MAC-Authentifizierung auf 802.1x-Authentifizierung
- FlexConnect mit 802.11u/Hotspot für mobile Netzwerke
- Standardbasiertes 802.11r Fast Roaming
- Bidirektionale Ratenbegrenzung (Durchsatzbegrenzungen pro Benutzer mit höherer Genauigkeit)
- VideoStream für Rich Media-Datenströme (im lokalen Modus)
- FlexConnect VLAN-basiertes zentrales Switching
- FlexConnect Split Tunneling
- Unterstützung für FlexConnect WGB/UWGB
- PPPoE-Client an einem AP
- NAT/PAT-Unterstützung an einem AP

Einige der neuen, in den 7.4-Code integrierten Features für Service Provider:

- LAG-Unterstützung (Link-Failover im Bruchteil einer Sekunde)
- 6 weitere Optionen für das RADIUS-Attribut des gesendeten Angerufenen-Station-ID hinzugefügt:ap-group-NameKartenstandortap-nameap-name-ssidflex-GruppennameVLAN-ID
- Sechs (6) weitere Optionen für die an einen DHCP-Server gesendete Option-82 hinzugefügt:ap-group-NameKartenstandortapname-vlan-idap-ethmac-ssidflex-Gruppennameapmac-vlan-id
- Konfigurierbare primäre und sekundäre RADIUS-Server auf FlexConnect-Gruppenebene; mit einer Begrenzung auf das Doppelte der auf der Plattform unterstützten FlexGroups (d. h. bis zu 4.000 RADIUS-Server auf einem 8500-Controller)

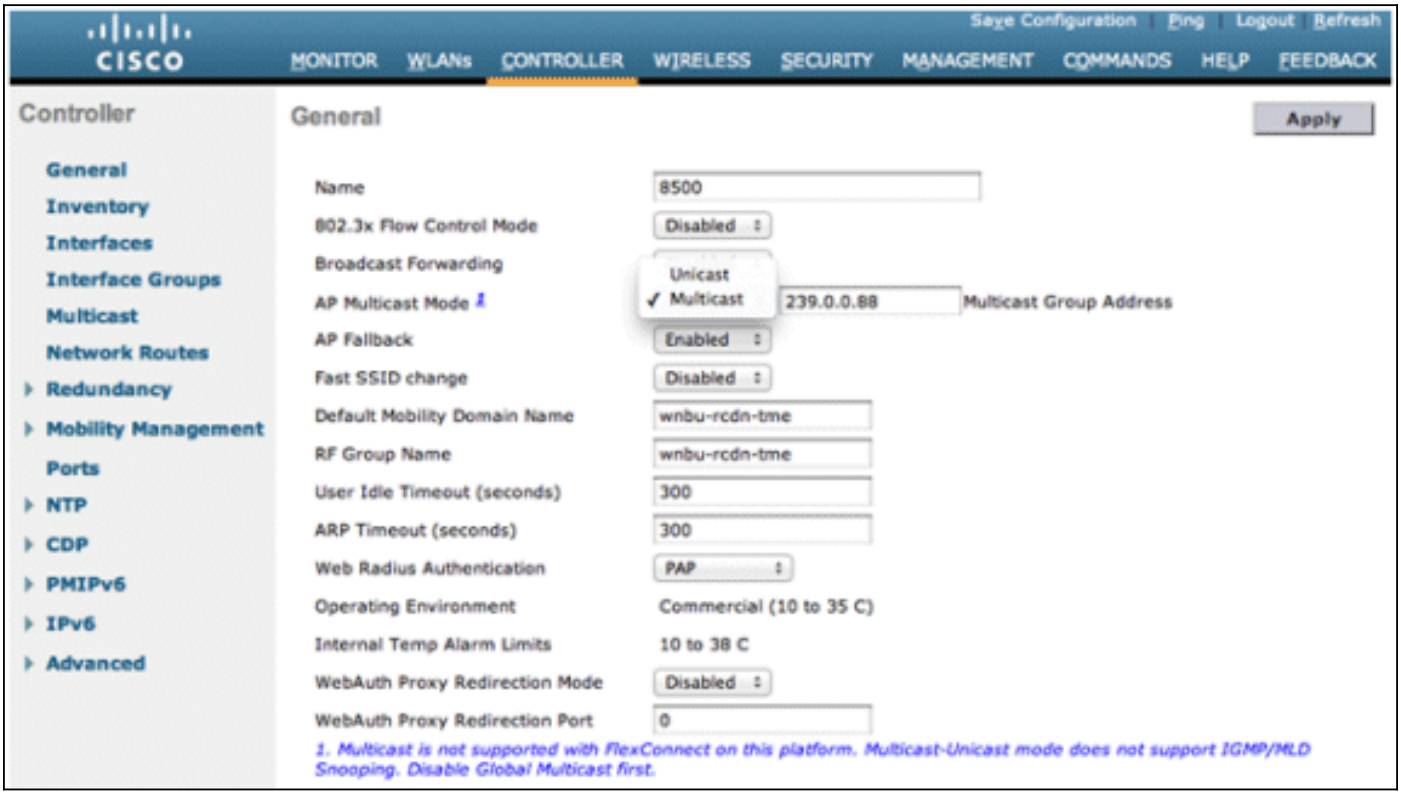
- Mehrere Controller-Managementverbesserungen (schnellerer HA-Upgrade-Prozess, SFTP-Dateiübertragungen, erweiterte Service-Port-Verfügbarkeit, präzise TACACS+-Kontrolle)
- Upstream-QoS (bidir-Client-Ratenbegrenzung)
- AP-Client-Lastenausgleich über AP-Ethernet-Nutzung
- DHCP-Proxymodus pro VLAN-Schnittstelle
- Mit HA-SKU bestellter WLC kann als Sekundär in einem "N+1"-Failover-Szenario verwendet werden (unterstützt die volle Plattformkapazität).
- AP-Funkmodule können so eingerichtet werden, dass sie nur 802.11n-Clients akzeptieren ("Nicht" ist mit "Grün" zu verwechseln).

Überlegungen zum Design

Multicast

Die Multicast-Unterstützung ist im Cisco Controller der Serie 8500 aktiviert, und der Betrieb ist mit dem der Cisco Controller der Serie 5500 vergleichbar, allerdings mit folgenden Einschränkungen:

1. Wenn alle APs auf dem 8500-Controller im lokalen Modus konfiguriert sind, ist Multicast-Multicast der Standardmodus, und alle Funktionen werden unterstützt (z. B. VideoStream). Dieses Szenario ist mit einem Controller der Serie 5500 identisch.
2. Wenn die APs als Mischung aus lokalem Modus und FlexConnect-Modus konfiguriert sind:Falls IPv6 auf den FlexConnect-APs erforderlich ist:Deaktivieren Sie den globalen Multicast-Modus, und wechseln Sie in den Multicast-Unicast-Modus.IPv6/GARP funktioniert auf FlexConnect- und Local-Mode-APs, Multicast-Daten und die VideoStream-Funktion werden jedoch deaktiviert.IPv6/GARP ist auf FlexConnect-APs nicht erforderlich:Ändern Sie den Modus in Multicast-Multicast, und aktivieren Sie Global Multicast Mode und IGMP/MLD Snooping.IPv6, GARP, Multicast Data und VideoStream werden von APs im lokalen Modus unterstützt.



Hinweis: Multicast-Unicast ist für den IPv6-Betrieb auf FlexConnect-APs (für RA- und NS-Paketübermittlung) erforderlich.

Plattformübergreifende Mobilität

In den meisten Netzwerken ist in der Regel die Unterstützung heterogener Wireless Controller in einer Mobilitätsgruppe erforderlich. Dabei kann es sich um Upgrade-, Migrations- oder Backup-Instanzen mit einer solch heterogenen Konfiguration handeln. In diesen Fällen sollte die Anzahl der unterstützten Fast Secure Roaming (FSR)-Clients im Netzwerkdesign berücksichtigt werden. Betrachten Sie beispielsweise ein großes Wireless-Netzwerk, das aus einer Kombination der folgenden WLC-Plattformen besteht, die alle in derselben Mobilitätsgruppe konfiguriert sind:

- 8500 (unterstützt FSR für 64.000 Clients)
- 7500 (unterstützt FSR für 64.000 Clients)
- WiSM2 (unterstützt FSR für 30.000 Clients)
- 5500 (unterstützt FSR für 14.000 Clients)

In diesem Szenario:

1. 64.000 authentifizierte Clients können nahtlos zwischen den 7500er und 8500er Jahren hin und her roamen.
2. 30.000 authentifizierte Clients können nahtlos zwischen mehreren WiSM2-Controllern oder zwischen einem WiSM2- bis 8500- oder 7500-Controller wechseln.
3. 14.000 authentifizierte Clients können nahtlos zwischen mehreren 5500 Controllern oder zwischen 5500 und einem WiSM2, 8500 oder 7500-Controller hin- und herwechseln.

Wireless-Clients, die diese Grenzwerte überschreiten, müssen nach Ablauf der Sitzungsüberschreitung erneut verbunden werden.

Lokale EAP-Authentifizierung

Die lokale EAP-Authentifizierungsdatenbank lässt sich nicht auf die unterstützten 64.000 Clients auf dem Controller 8500 skalieren. Obwohl die 8500-Funktion als Authentifizierungsserver in der

Benutzeroberfläche nicht deaktiviert wurde, dient sie lediglich der Unterstützung der Testeinrichtung und **nicht** der Produktionsbereitstellung.

Link-Aggregation (LAG)

Die LAG der 2x10G-Schnittstellen wird in den Softwareversionen 7.4 und höher unterstützt. Die LAG-Konfiguration ermöglicht einen Aktiv/Aktiv-Verbindungsbetrieb mit schneller Failover-Link-Redundanz.

Hinweis: Der zusätzliche aktive 10G-Link ändert den gesamten Netzwerkdurchsatz des Controllers nicht.

Zugehörige Informationen

- Wi-Fi-Lösung für Service Provider - Überblick
- Cisco Prime-Infrastruktur 1.2
- CUWN Softwareversion 7.3
- Technischer Support und Dokumentation - Cisco Systems