Migrationsleitfaden für WLSM der Catalyst Serie 6500 zu Catalyst WiSM der Serie 6500

Inhalt

Einführung

Im Mittelpunkt dieses Dokuments steht die Migrationsstrategie von einem vorhandenen Wireless LAN Services Module (WLSM) zu einem Wireless Services Module (WiSM). Bei der Migration vom Cisco WLSM zum Cisco WiSM ist eine sorgfältige Planung und Durchführung unbedingt erforderlich.

Die Zielgruppe für dieses Dokument sind Netzwerkmanager von Unternehmen und Einzelpersonen auf allen Ebenen der IT-Infrastruktur eines Unternehmens, die an der Planung, Implementierung oder Wartung der WLSM-basierten Wireless-Netzwerke beteiligt sind. Sekundäre Zielgruppe sind Personen, die Produkte und Integrationsservices bereitstellen oder IT-Abteilungen in Unternehmen unterstützen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst WLSM der Serie 6500
- Cisco Catalyst WiSM der Serie 6500

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).

Übersicht

Eine Migrationsstrategie vom Catalyst WLSM zur Catalyst WiSM-Plattform umfasst die Planung und Durchführung folgender Maßnahmen:

- Planen und installieren Sie Catalyst WiSM.
- Installieren Sie die Catalyst WiSM-Plattform.
- Installieren Sie die Netzwerkverwaltungsplattform des Cisco Wireless Control System (WCS) für Catalyst WiSM.
- Migrieren Sie die Konfigurationen vom Catalyst WLSM zur Catalyst WiSM-basierten Plattform, um die Unterstützung aller leichten und konvergenten autonomen Access Points aufrechtzuerhalten.
- Migrieren Sie die autonomen IOS® Access Points auf die LWAPP-fähige IOS-Plattform (außerhalb des Anwendungsbereichs des Dokuments).
- Schulung der Support-Mitarbeiter für die Catalyst WiSM-Plattform und -Lösung
- Säubern Sie die vorhandenen Konfigurationen, wenn die Migration abgeschlossen ist.

Unterschiede in der Architektur

Cisco Catalyst WLSM der Serie 6500

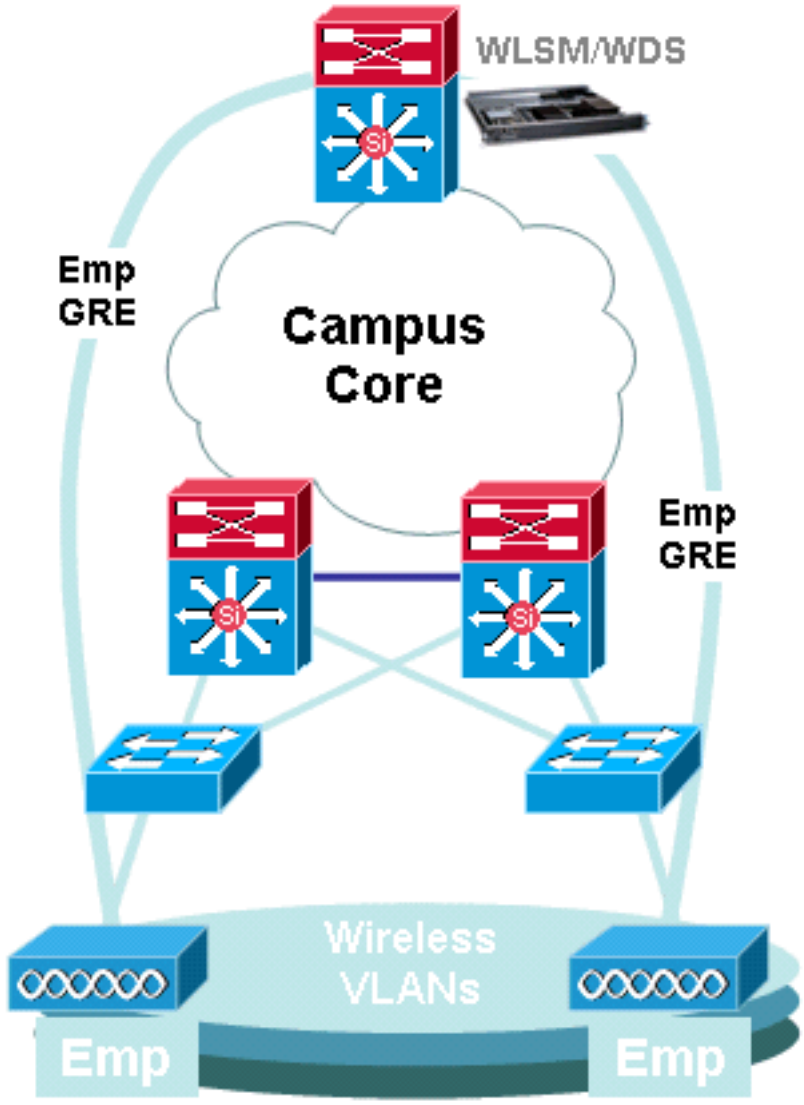
Der Cisco Catalyst WLSM der Serie 6500 kann in jedem freien Steckplatz eines Cisco Catalyst Switches der Serie 6500 mit 3, 6, 9 oder 13 Steckplätzen installiert und konfiguriert werden, der mit der Supervisor Engine 720 ausgestattet ist. Der WLSM der Cisco Catalyst Serie 6500 arbeitet mit autonomen Cisco Aironet Access Points und der Cisco Works Wireless LAN Solution Engine (WLSE) zusammen.

Der Cisco Catalyst WLSM der Serie 6500 wird in der Regel im Distribution Layer oder im Rechenzentrum eingesetzt. Sie wird selten im Verteilerschrank eingesetzt. Ein unabhängiger

Access Point ist mit jedem Switch-Port in einem Layer-3-Netzwerk verbunden. Upstream-Switches oder -Router müssen nicht konfiguriert werden, und es sind keine spezifische VLAN-Zuweisung oder Trunks erforderlich. Bevor Datenverkehr aktiv weitergeleitet wird, kann der autonome Access Point als vertrauenswürdiges Netzwerkgerät authentifiziert werden.

Eines der wichtigsten Konzepte, das mit der Verwendung des WLSM eingeführt wurde, ist die Mobilitätsgruppe. Ein Wireless-Client erfährt nahtloses Roaming (behält alle IP-Sitzungen bei), wenn er zwischen zwei Access Points wechselt, die als Teil derselben Mobilitätsgruppe konfiguriert wurden. Eine Mobilitätsgruppe wird auf dem Access Point durch eine eindeutige Zuordnung zwischen dem Service Set Identifier (SSID) für die Funkseite und der Netzwerk-ID für die kabelgebundene Seite definiert. Die Netzwerk-ID stellt das Overlay-logische Netzwerk dar, das auf der vorhandenen Infrastruktur mithilfe von GRE-Tunneln (Generic Routing Encapsulation) aufgebaut ist. Durch seine Zuordnung zur SSID wird dies zwischen der SSID und der VLAN-ID ersetzt.

Weitere Informationen zur Konfiguration und Bereitstellung des WLSM finden Sie im Bereitstellungsleitfaden für das Cisco Catalyst Wireless LAN Services Module (WLSM) der Serie 6500.



Beachten Sie, dass jedem SSID immer noch ein VLAN zugeordnet ist. Diese VLANs sind jetzt nur noch für den Access Point definiert und müssen nicht auf den Switches des Access-Layers oder des Distribution-Layers konfiguriert werden. Der einzige Zweck des VLAN-Teils der Konfiguration

besteht darin, eine Bindung zwischen der mit dem VLAN verknüpften Verschlüsselung an eine bestimmte SSID bereitzustellen.

```
dot11 vlan-name Emp vlan 3
!
dot11 ssid Employee
 vlan 3
 authentication open eap
eap_methods
 authentication network-eap
eap_methods
 authentication key-management
wpa
 mobility network-id 3
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 3 mode ciphers
tkip
 !
 ssid Employee
```

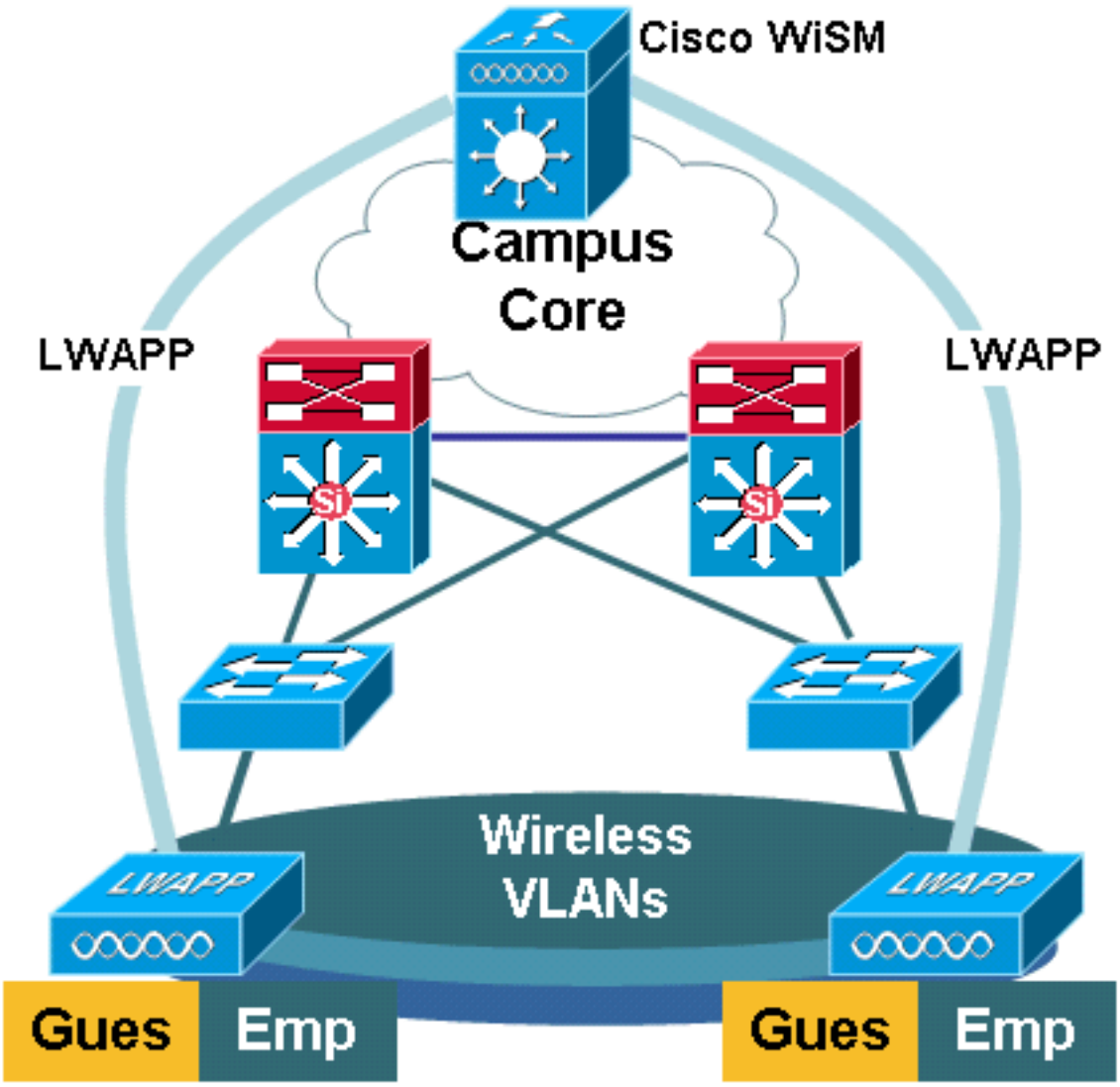
```
interface Tunnel3
 description mGRE for
employees
 ip address 10.10.3.1
255.255.255.0
 no ip redirects
 ip mtu 1476
 ip dhcp snooping
packets
 tunnel source
Loopback3
 tunnel mode gre
multipoint
 mobility network-id 3
!
```

Cisco Catalyst WiSM der Serie 6500

Das Cisco Catalyst WiSM der Serie 6500 gehört zur Cisco Wireless LAN Controller (WLC)-Produktfamilie, die auch Cisco Unified Wireless Networks genannt wird. Das Cisco WiSM arbeitet mit Cisco Aironet Lightweight Access Points (LAPs) und dem Cisco WCS zusammen. Das Cisco WiSM lässt sich nahtlos in vorhandene Cisco Catalyst Enterprise Networks der Serie 6500 integrieren. Sie ist skalierbar, um einen sicheren, unternehmensweiten Wireless-Zugriff für Hauptniederlassungen, Zweigstellen und Remote-Standorte bereitzustellen. Die Kommunikation erfolgt über LWAPP, um sichere Verbindungen zwischen Access Points und Modulen in Layer-3-Netzwerken herzustellen. Aus Sicht der Datenverkehrsverwaltung wird der gesamte Datenverkehr von den mit den LAPs verknüpften Wireless-Clients von den Access Points selbst gekapselt und an einen WLC übertragen, der den Datenverkehr aggregiert und den Ein- und Ausgangs-Punkt für IP-Datenverkehr zum und vom kabelgebundenen Netzwerk darstellt.

Diese Unterschiede bestehen jedoch:

- Der Datenverkehr wird von den Access Points zum zentralen Controller getunnelt, der LWAPP und nicht GRE nutzt.
- Steuerung und Datenverkehr werden über LWAPP übertragen. Datenverkehr verwendet UDP-Port 1222, Steuerungsdatenverkehr wird in UDP-Port 12223 gekapselt, und Mobilitätsnachrichten verwenden die UDP-Ports 1666/1667.
- Der Kontrolldatenverkehr ist mit Advanced Encryption Standard (AES) verschlüsselt, und die Daten sind klar.
- Es gibt keinen separaten logischen Tunnel für jede definierte SSID. Zwischen jedem Access Point und dem WLC wird nur ein einziger logischer Tunnel erstellt. Dieser LWAPP-Tunnel wird verwendet, um den Datenverkehr für alle mit dem Access Point verbundenen Wireless-Clients zu übertragen, unabhängig davon, mit welchem SSID diese verbunden sind.



Migrationsstrategie

Produkt-Software aktualisieren

Aktualisieren Sie die Software für die folgenden Produkte:

- Der Supervisor 720 muss die Cisco IOS Software Version 12.2(18)SXF2 oder höher ausführen.
- Catalyst 6500 WLSM muss ab Version 1.4.1 ausgeführt werden.
- Catalyst 6500 WiSM muss 3.2.78.4 oder höher ausführen
- Cisco Aironet Access Points müssen die Cisco IOS Software Version 12.3.7JA2 oder höher ausführen (um in LWAPP umgewandelt zu werden).

Implementieren von Konfigurationen

Implementieren Sie diese Konfigurationen:

- Konfigurieren Sie den Supervisor 720 so, dass er das Cisco WiSM unterstützt.

- Konfigurieren Sie das VLAN für die WiSM-Verwaltungsschnittstelle auf dem Supervisor 720.
- Konfigurieren Sie das VLAN für die dynamische Schnittstelle des WiSM auf dem Supervisor 720.
- Konfigurieren Sie DHCP so, dass der Bereich für die Dienstschnittstelle festgelegt wird, oder konfigurieren Sie die IP-Adresse statisch.
- Testen Sie die neuen Layer-3-Netzwerke auf Routing-Probleme.

Weitere Informationen zum Abschließen dieser Konfigurationen finden Sie im Cisco WiSM-Konfigurationshandbuch und in der Fehlerbehebung und Konfiguration der WiSM-Einrichtung (Initial Wireless Services Module).

Konfigurieren des Catalyst 6500 WiSM zur Migration der SSID vom Catalyst 6500 WLSM

Im Fall der Cisco WLSM-Architektur wird die auf einem Access Point konfigurierte SSID einem Mobilitätsnetzwerk zugeordnet, das den gesamten Client-Datenverkehr an den Catalyst 6500 weiterleitet. Diese Multipoint-GRE-Tunnel (mGRE) verfügen über einen einzigen Terminationspunkt auf dem Supervisor 720-Modul des Catalyst 6500, das das WLSM hostet. Der andere logische Endpunkt des Tunnels ist auf allen Zugangspunkten vorhanden, die Teil des Layer-3-Mobilitätsnetzwerks sind. Bei einer Cisco WiSM-Plattform wird die SSID als WLAN dargestellt. Jedes WLAN ist der Verwaltungsschnittstelle oder einer vom Bediener definierten dynamischen Schnittstelle zugeordnet. Die vom Bediener definierten dynamischen Schnittstellen entsprechen VLANs und fungieren als DHCP-Relay für Wireless-Clients.

Für jede Mobilitätsgruppe muss auf dem Supervisor 720-Modul ein mGRE-Tunnel definiert werden. Das Beispiel zeigt eine mGRE-Tunnelschnittstelle auf einem Supervisor 720. Alle Wireless-Clients verwenden die IP-Adresse der Tunnelschnittstelle als Standard-Gateway. Die Mobility-Netzwerk-ID definiert dies als ein einzigartiges Mobilitätsnetzwerk. Die für diesen Tunnel definierte Mobility-Netzwerk-ID wird ebenfalls unter einer der SSID-Definitionen für den Access Point definiert, um seine Beteiligung an diesem Layer-3-Mobilitätsnetzwerk zu ermitteln.

Hinweis: Eine Mobilitätsgruppe ist eine Gruppe von Wireless-Clients, die für einige gemeinsame Merkmale gruppiert sind, z. B. ein gemeinsames Authentifizierungs- oder Verschlüsselungsschema, oder Benutzertypen, wie z. B. Besucher und Mitarbeiter.

Diese Ausgabe zeigt die Konfiguration auf dem Supervisor 720:

```
interface Tunnel172
 description to_wireless_clients
 ip address 172.16.1.1 255.255.255.0
 ip helper-address 10.1.1.11
 no ip redirects
 ip dhcp snooping packets
 tunnel source Loopback100
 tunnel mode gre multipoint
 mobility network-id 172
```

Diese Ausgabe zeigt die entsprechende Konfiguration für den Access Point:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 172 mode ciphers tkip
```

```
!
ssid light
   vlan 172
   authentication network-eap eap_methods
   authentication key-management wpa
   mobility-network-id 172
```

Um diese Konfiguration in die WiSM-Architektur umzuwandeln, müssen Sie eine neue dynamische/VLAN-Schnittstelle erstellen, ihr eine IP-Adresse in einem anderen Subnetz zuweisen und sie einem WLAN zuordnen.

Der Name der WLAN-Schnittstelle entspricht dem SSID-Namen der Cisco Aironet Access Points. In diesem Beispiel ist es "light". Wenn Sie einen ähnlichen Namen beibehalten, ist die Benutzerfreundlichkeit minimal. Der einzige Unterschied ist das IP-Adresssegment, aus dem den Wireless-Clients eine IP-Adresse zugewiesen wird.

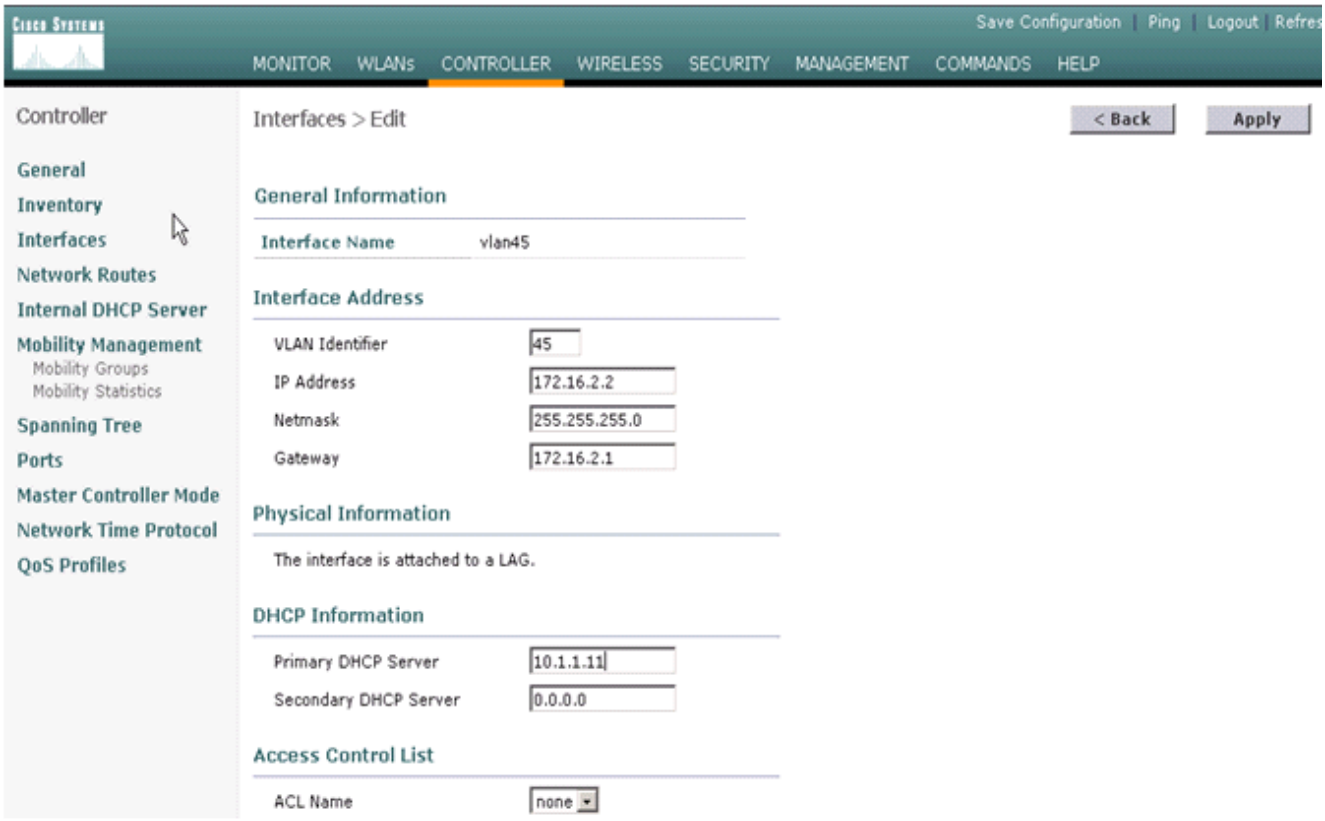
1. Erstellen Sie das neue VLAN im Supervisor 720, und fügen Sie es der VLAN-Datenbank hinzu.
   ```
   c6506-t(config)#interface vlan 45
   c6506-t(config-if)#ip add 172.16.2.1 255.255.255.0
   c6506-t(config-if)#no shut
   c6506-t(config-if)#end
   c6506-t(config)#vlan 45
   c6506-t(config-vlan)#state active
   c6506-t(config-if)#end
   ```

2. Erlauben Sie das VLAN in den Trunked Gigabit-Schnittstellen.
   ```
   c6506-t(config)#interface range gig 1/1-4
   c6506-t(config-if-range)#switchport mode trunk
   c6506-t(config-if-range)#switchport trunk encap dot1q
   c6506-t(config-if-range)#switchport trunk native vlan 201
   c6506-t(config-if-range)#switchport trunk allowed vlan 201,45
   c6506-t(config-if-range)#mls qos trust dscp
   c6506-t(config-if-range)#spanning-tree portfast
   c6506-t(config-if-range)#channel-group 1 mode on
   c6506-t(config-if-range)#end
   ```

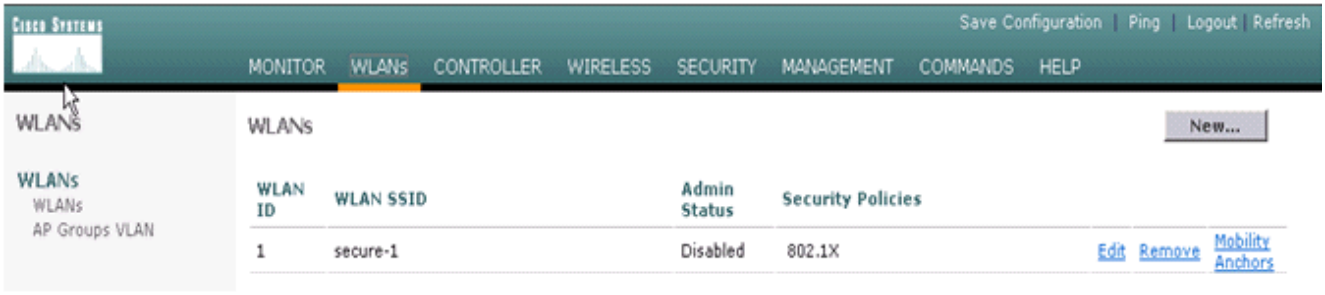
3. Sobald das VLAN in der Trunk-Schnittstelle zugelassen ist, wird es automatisch in der Port-Channel-Schnittstelle zugelassen.
   ```
   c6506-t#show run interface port-channel 1
   !
   interface Port-channel1
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 201
    switchport trunk allowed vlan 45,201
    switchport mode trunk
    no ip address
   end
   c6506-t#
   ```
4. Führen Sie diese Schritte aus, um die dynamische Schnittstelle im Catalyst 6500 WiSM über die Webschnittstelle zu erstellen.Wählen Sie **Controller > Interfaces (Controller > Schnittstellen)** und klicken Sie auf **New**.

Geben Sie einen Schnittstellennamen und eine VLAN-ID ein, und klicken Sie auf **Übernehmen**.

Geben Sie die entsprechenden IP-Adressinformationen und die DHCP-Serverinformationen ein, und klicken Sie auf **Übernehmen**.

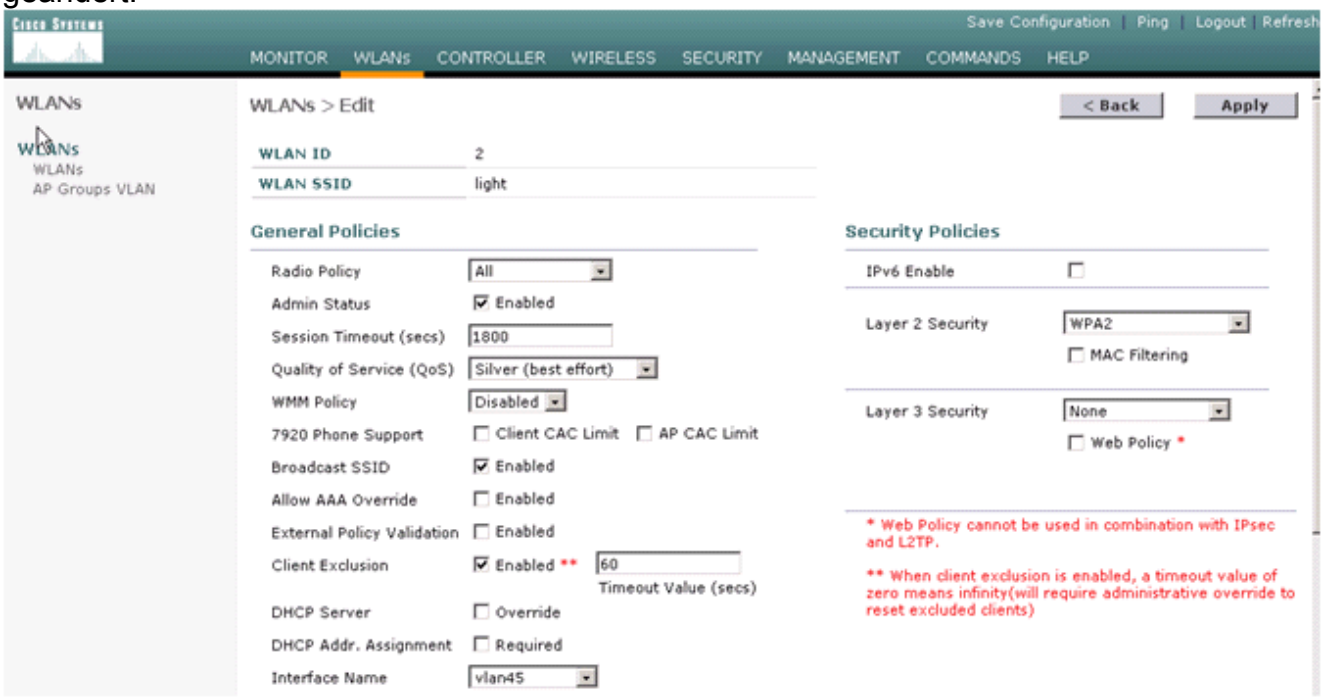


Wählen Sie **WLANs aus**, und klicken Sie auf **Neu**, um eine neue SSID für Cisco WiSM hinzuzufügen.



Fügen Sie die SSID-**LED hinzu**, und klicken Sie auf **Übernehmen**.

Ändern Sie den Parameter für den Schnittstellennamen in das entsprechende VLAN.Andere Sicherheitsparameter, z. B. der entsprechende RADIUS-Server und die Verschlüsselungseinstellungen, müssen der Konfiguration des unabhängigen Cisco Access Points entsprechen. In diesem Beispiel wird der Schnittstellenname in **VLAN45** geändert, und der Sicherheitstyp für Layer 2 wird in **WPA2** geändert.



Hier ist das neue SSID-Licht.

Wenn eine neue SSID verwendet wird, sind keine weiteren Konfigurationen erforderlich. Wenn eine vorhandene SSID verwendet wird, aktualisieren Sie jeweils nur eine RF-Domäne,

um Mobilitätsprobleme zwischen dem Catalyst 6500 WSLM und dem Catalyst 6500 WiSM zu vermeiden.Überprüfen Sie nach der Konfiguration der WLANs, ob die WLAN-Richtlinien korrekt sind. Beispielsweise ACL, QoS usw.Stellen Sie sicher, dass das Cisco WCS betriebsbereit ist und für die Verwaltung des Cisco WiSM konfiguriert werden kann.

LWAPP-Umwandlung des Access Points

Die Migration vom autonomen Access Point-Modus zum Lightweight-Modus ist auf den folgenden Cisco Aironet Access Point-Plattformen möglich:

- Alle Cisco Aironet Access Points der Serie 1130 AG
- Alle Cisco Aironet Access Points der Serie 1240 AG
- Bei allen IOS-basierten modularen Access Points der Serie 1200 (Cisco IOS Software Upgrade, 1210 und 1230 AP-Plattformen mit 1200/1220) hängt dies vom Funkmodul ab:Wenn 802.11G, MP21G und MP31G unterstützt werdenwenn 802.11A, CB21A und CB22A unterstützt werden
- Die Cisco Aironet Access Points der Serie 1200 können mit einer beliebigen Kombination von unterstützten Funkmodulen aufgerüstet werden - nur G, A oder sowohl G als auch A.

. Access Points müssen die Cisco IOS Software Version 12.3(7)JA oder höher ausführen, bevor Sie das Upgrade durchführen können. Weitere Informationen zum Umwandlungsverfahren finden Sie unter Upgrade autonomer Cisco Aironet Access Points auf Lightweight Mode.

Access Point-Verteilung zwischen Controllern im Cisco WiSM

Wenn ein Access Point bereits mit einer statischen IP-Adresse konfiguriert ist, behält der Access Point die IP-Adresse bei, nachdem er aus dem autonomen Modus in den LWAPP-Modus konvertiert wurde. Wenn sich der Access Point nicht im selben IP-Subnetz wie der Controller befindet, ist die DNS-Auflösung von CISCO-LWAPP-CONTROLLER@localdomain der einzige garantierte Mechanismus zur Controller-Erkennung. Das Upgrade-Dienstprogramm kann einen Namenserver konfigurieren, bevor Sie die Cisco IOS Software Version 12.3(7)JX laden. Stellen Sie sicher, dass der Name-Server CISCO-LWAPP-CONTROLLER@localdomain ordnungsgemäß auflösen kann, bevor Sie mit dem Upgrade beginnen.

Sie können auch die anbieterspezifische DHCP-Option 43 verwenden, um eine oder mehrere Controller-IP-Adressen an einen Access Point in der DHCP-Angebotsmeldung zurückzugeben. Der Access Point sendet eine LWAPP-Erkennungsmeldung an die Management-IP-Adresse des Controllers, den er in der DHCP-Option 43 empfängt. Siehe Anhang A: Konfigurieren der DHCP-Option 43 für Lightweight Cisco Aironet Access Points auf Windows 2003 Enterprise DHCP Server für weitere Informationen zum Konfigurieren der DHCP-Option 43 in einem Windows 2003 Enterprise DHCP Server.

Test mit einer begrenzten Anzahl von Access Points

Starten Sie den Migrationsprozess mit einem einzigen Access Point an einem für den Administrator leicht zugänglichen Ort, und versuchen Sie dann, einen Remote-Standort einzurichten. Nachdem die Access Points in den LWAPP-Modus konvertiert wurden und die Cisco WiSM-Konfiguration abgeschlossen ist, testen Sie die Wireless-Clients auf Folgendes:

- Sicherheitseinstellungen
- Standardanwendungen wie E-Mail, Internetzugang, Datenbankanwendungen usw.

- Reibungsloses Roaming zwischen Access Points und Überprüfung, ob die Clients die IP-Adressen beim Roaming zwischen Access Points behalten
- Beliebige Probleme mit der maximalen Segmentgröße (Maximum Segment Size, TCP) - Laden Sie große Internetseiten herunter oder übertragen Sie Dateien über File Transfer Protocol (FTP).
- Akzeptierbarer Durchsatz der Wireless Access Points gemäß Design

Vollständige Bereitstellung

Um sich schnell durch größere Access Point-Nummern zu bewegen, installieren Sie das Upgrade-Utility auf mehr als einem Rechner für die gleichzeitige Konvertierung mehrerer autonomer Access Points zu LWAPP-fähigen Access Points.

Fehlerbehebung

Bei spezifischen Problemen im WLC befolgen Sie die normalen Fehlerbehebungsverfahren. Weitere Informationen zur Fehlerbehebung finden Sie in den Häufig gestellten Fragen zur Fehlerbehebung für den Wireless LAN Controller (WLC).

Zugehörige Informationen

- Unterstützung von WLAN-Technologie
- Tipps zur Fehlerbehebung beim LWAPP-Upgrade-Tool
- Konfigurationshinweis für das Catalyst Wireless LAN Services Module der Serie 6500
- Cisco Catalyst Wireless LAN Services Module der Serie 6500 - Fragen und Antworten
- Technischer Support und Dokumentation - Cisco Systems