

Cisco Mobility Services Engine - Implementierungsleitfaden für kontextsensitive Mobilitätslösungen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Abschnitt 1: Lösungsüberblick](#)

[Terminologie](#)

[Technologie-Hintergrundinformationen](#)

[RSSI \(Signalstärke-Indikation empfangen\)](#)

[TDOA \(Zeitdifferenz der Ankunft\)](#)

[Aktive RFID-Tags](#)

[Abschnitt 2: Planung und Einrichtung Ihres kontextsensitiven Netzwerks](#)

[Positionierung des Access Points](#)

[Tracking Optimized Monitor Mode \(TOMM\)](#)

[Platzierung von APs und Antennen](#)

[Signaldämpfung](#)

[Überwachung von Mehrstöckigen Gebäuden, Krankenhäusern und Lagerhäusern](#)

[Standortrollen und Regionen](#)

[Erstellen einer Maske im System Manager](#)

[Zellen in kontextsensitiver Engine für Tags](#)

[Erstbetrieb bei Zellenkonfiguration](#)

[Kalibrierung - kontextsensitive Engine für Clients](#)

[Exciter \(Chokepoint Trigger\)-Technologie](#)

[Überlegungen zur Bereitstellung kontextsensitiver Informationen mit vorhandenen Daten- und Sprachdiensten](#)

[Allgemeine Richtlinien - TDOA](#)

[Kabelgebundener Standort](#)

[Abschnitt 3: Validierung und Verbesserung Ihres kontextsensitiven Netzwerks](#)

[WCS Accuracy Tool](#)

[Tool zur Standortbereitschaft](#)

[Kontextsensitiv - Systemleistung](#)

[RFID-Tag und WLC-Konfiguration/-Optimierung](#)

[Konfiguration und Optimierung von WCS und MSE](#)

[Fehlerbehebung](#)

[Abschnitt 4: Finale Checkliste](#)

[Hardware-Anforderungen](#)

[Abschnitt 5: Häufig gestellte technische Fragen](#)

[Anhang A: MSE-Einrichtung](#)

[MSE zum WCS hinzufügen](#)

[Anhang B: WLC- und MSE-Befehle](#)

[Anhang C: MSE-Upgrade von 5.x auf 6.0](#)

[Anhang D: MSE-Datenbankwiederherstellung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält Richtlinien für Konfiguration und Bereitstellung sowie Tipps zur Fehlerbehebung und Antworten auf häufig gestellte technische Fragen für diejenigen, die die Cisco Mobility Services Engine (MSE) hinzufügen und kontextsensitive Services zu einem Cisco Unified WLAN ausführen. Ziel dieses Dokuments ist es,

- Erläutern der verschiedenen Elemente und des Frameworks für die Cisco Mobility-Lösung
- Bereitstellung allgemeiner Richtlinien für die Bereitstellung der Cisco Mobility-Lösung

Dieses Dokument enthält keine Konfigurationsdetails für die MSE und die zugehörigen Komponenten. Diese Informationen werden in anderen Dokumenten bereitgestellt und Referenzen werden bereitgestellt. Im Abschnitt [Zugehörige Informationen](#) finden Sie eine Liste von Dokumenten zur Konfiguration und zum Design von kontextsensitiven Mobilitätsdiensten. Die adaptive WIPS-Konfiguration wird in diesem Dokument ebenfalls nicht behandelt.

[Voraussetzungen](#)

[Anforderungen](#)

Es gibt keine spezifischen Anforderungen für dieses Dokument.

[Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

[Konventionen](#)

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

[Hintergrundinformationen](#)

Die Cisco MSE ermöglicht die Überwachung des physischen Standorts von kabelgebundenen und Wireless-Netzwerkgeräten mithilfe von Wireless LAN-Controllern (WLCs) und Cisco Aironet Lightweight Access Points (LAPs). Mit dieser Lösung kann ein Kunde alle Wi-Fi-Geräte verfolgen, einschließlich Clients, aktive RFID-Tags und nicht autorisierte Clients und Access Points (APs).

Bei der Entwicklung wurden folgende Anforderungen berücksichtigt:

- **Verwaltbarkeit** - Das Cisco Wireless Control System (WCS) dient zum Verwalten und Überwachen der MSE. Darüber hinaus lässt sich die MSE direkt in die Wireless LAN-Architektur integrieren, die anstelle mehrerer unterschiedlicher Wireless-Netzwerke ein einheitliches Netzwerk für die Verwaltung bereitstellt.
- **Skalierbarkeit** - Die Cisco MSE-Serie kann bis zu 18.000 Netzwerkelemente gleichzeitig nachverfolgen. Das WCS kann mehrere Mobility Services Engines verwalten, um die Skalierbarkeit zu erhöhen. Controller, WCS und MSE werden über separate Geräte implementiert, um eine höhere Skalierbarkeit und Leistung zu ermöglichen.
- **Sicherheit** - Der MSE, WCS und der Wireless LAN Controller bieten robuste, sichere Schnittstellen und sichere Protokolle für den Zugriff auf Daten. Die MSE zeichnet Verlaufsstandortinformationen auf, die für Prüfpfade und die Einhaltung von Vorschriften verwendet werden können.
- **Offen und standardbasiert** - Die MSE verfügt über eine SOAP/XML-API, auf die externe Systeme und Anwendungen zugreifen können, die Standortinformationen von der MSE nutzen können.
- **Einfache Bereitstellung von Geschäftsanwendungen:** Die MSE kann in neue Geschäftsanwendungen wie Ressourcenverfolgung, Bestandsmanagement, standortbasierte Sicherheit oder automatisiertes Workflow-Management integriert werden.

Dieses Dokument ist in fünf Abschnitte unterteilt:

1. [Lösungsüberblick](#)
2. [Kontextsensitive Planung und Einrichtung eines Wi-Fi-Netzwerks](#)
3. [Validierung und Optimierung kontextsensitiver Netzwerke](#)
4. [Fehlerbehebung](#)
5. [Endgültige Check-Artikel](#)

[Abschnitt 1: Lösungsüberblick](#)

Der Context Aware Service (CAS) bietet die Möglichkeit für ein Wi-Fi 802.11a/b/g/n-Netzwerk, den Standort einer Person oder eines Objekts mit einem aktiven Wi-Fi-Gerät zu bestimmen, z. B. einen Wireless-Client oder ein aktives RFID-Tag und/oder zugehörige Daten, die vom Endpunkt über die Wireless-Infrastruktur an einen Upstream-Client weitergeleitet werden können. Wenn eine Cisco Mobility Service Engine (MSE) zu einem Cisco Unified Wireless Network (CUWN) mit einer entsprechend lizenzierten Version von WCS hinzugefügt wird, übernimmt sie die Verantwortung für mehrere wichtige Aufgaben:

- Ausführung von Positionierungsalgorithmen
- Pflege der Kalibrierinformationen
- Trigger und Versand von Standortbenachrichtigungen
- Statistikprozess und historische Lage
- Depot für geografische Informationen, Karten und alle Wireless-Geräte

WCS ist das Managementsystem, das mit der MSE interagiert und Benutzeroberflächen (UI) für die von der MSE bereitgestellten Dienste bereitstellt. Obwohl der direkte Zugriff auf die MSE zu Wartungs- und Diagnosezwecken über SSH oder eine Konsolensitzung möglich ist, wird die gesamte Interaktion zwischen Benutzer und Bediener und MSE in der Regel über WCS (für die Verwaltung) oder eine Client-Anwendung eines Drittanbieters ausgeführt.

Terminologie

Mit der zentralen Cisco Wireless LAN-Architektur und kontextsensitiven Standortdiensten können Administratoren den Standort eines 802.11-basierten Geräts sowie den Typ oder Status jedes Geräts bestimmen. Clients (zugeordnete Clients, Suchvorgänge usw.), nicht autorisierte Access Points, nicht autorisierte Clients und aktive Tags können vom System identifiziert und lokalisiert werden. Diese Informationen werden innerhalb von Sekunden nach dem Auftreten eines Ereignisses über die API bereitgestellt und können von der MSE-Datenbank für Verlaufssuchen oder Sicherheitsprüfungen aufbewahrt werden.

Mobility Services Engine (MSE): MSE unterstützt eine Reihe von Mobilitätsservices. Die MSE ist als offene Plattform konzipiert und unterstützt Software für Mobilitätsdienste modular mit verschiedenen Konfigurationsoptionen, die auf der Netzwerktopologie und den erforderlichen Servicetypen basieren. Der Wert der MSE wird durch die verschiedenen Mobilitätsservices-Anwendungen bereitgestellt. Cisco unterstützt vorhandene und zukünftige Software, darunter:

- **Kontextsensitive Services:** Diese Programme erfassen und integrieren detaillierte Kontextinformationen über z. B. Standort, Temperatur, Verfügbarkeit und verwendete Anwendungen in Geschäftsprozesse. Kontextbewusste Anwendungen bieten eine Vielzahl von Standortoptionen, darunter Standort in Echtzeit, Erkennen von Erreichbarkeitsanzeige, Sichtbarkeit von Treffpunkten und Telemetrie. Die Unterstützung von RSSI (Received Signal Strength Indication) und TDoA (Time Difference of Arrival) sorgt für eine höhere Genauigkeit und Leistung bei der Skalierung in einer Vielzahl von Umgebungen. Kontextbewusste Software besteht aus zwei Hauptkomponenten:
Kontextsensitive Engine für Clients: Die Cisco Location Engine (RSSI) dient der Verfolgung von Wi-Fi-Clients, nicht autorisierten Clients, nicht autorisierten APs und kabelgebundenen Clients.
Kontextsensitive Engine für Tags: Die Partner (AeroScout) Location Engine (sowohl RSSI als auch TDOA) dient der Verfolgung aktiver Wi-Fi-RFID-Tags. Anwendungen von Drittanbietern werden durch die MSE API unterstützt.
- **Adaptive Wireless Intrusion Prevention System (wIPS):** wIPS-Software bietet Transparenz und umfassenden Schutz vor Bedrohungen für das Mobilitätsnetzwerk durch Überwachung, Warnmeldungen, Klassifizierung und Behebung von Schwachstellen in Wireless- und kabelgebundenen Netzwerken.

Network Mobility Services Protocol: Cisco-definiertes Protokoll, das für die sichere Kommunikation zwischen dem WLC und der MSE verwendet wird.

Wireless Control System (WCS): Von Cisco Systems entwickelte und unterstützte Wireless-Netzwerkmanagementsysteme. Beinhaltet folgende Funktionen:

- WLAN-Konfiguration
- WLAN-Leistungsüberwachung
- Reporting (Echtzeit- und Verlaufsberichte)
- Grafische Ansicht des Netzwerks (Wireless LAN-Controller, Access Points, Clients und Tags)

Wireless LAN Controller (WLC): Die CUWN-Architektur zentralisiert die WLAN-Konfiguration und -Steuerung in einem Gerät, das als WLAN-Controller (WLC) bezeichnet wird. Dadurch kann das gesamte WLAN als intelligentes Netzwerk betrieben werden, das Wireless als Zugangsmittel zur Unterstützung erweiterter Services verwendet. Dies unterscheidet sich von älteren 802.11-WLAN-Infrastrukturen, die aus autonomen, eigenständigen Access Points aufgebaut sind. Das CUWN vereinfacht das Betriebsmanagement, indem eine große Anzahl verwalteter Endpunkte (autonome Access Points) in einem einzigen verwalteten System zusammengefasst wird, das aus

den WLAN-Controllern und den zugehörigen, miteinander verbundenen Access Points besteht.

In der CUWN-Architektur sind APs "leicht", d. h. sie können nicht unabhängig von einem WLC agieren. APs werden in der Regel ohne Benutzereingriff bereitgestellt, und es ist keine individuelle Konfiguration der APs erforderlich. Die APs erfassen die IP-Adresse eines oder mehrerer WLC über einen Controller-Erkennungsalgorithmus und stellen dann über einen "Join"-Prozess eine Vertrauensbeziehung zu einem Controller her. Sobald die Vertrauensbeziehung hergestellt ist, überträgt der WLC ggf. die Firmware an den Access Point und eine Laufzeitkonfiguration. APs speichern eine Konfiguration nicht lokal.

Clients: Alle Geräte, die Controller-basierten Lightweight Access Points in einem Wireless-Netzwerk zugeordnet sind.

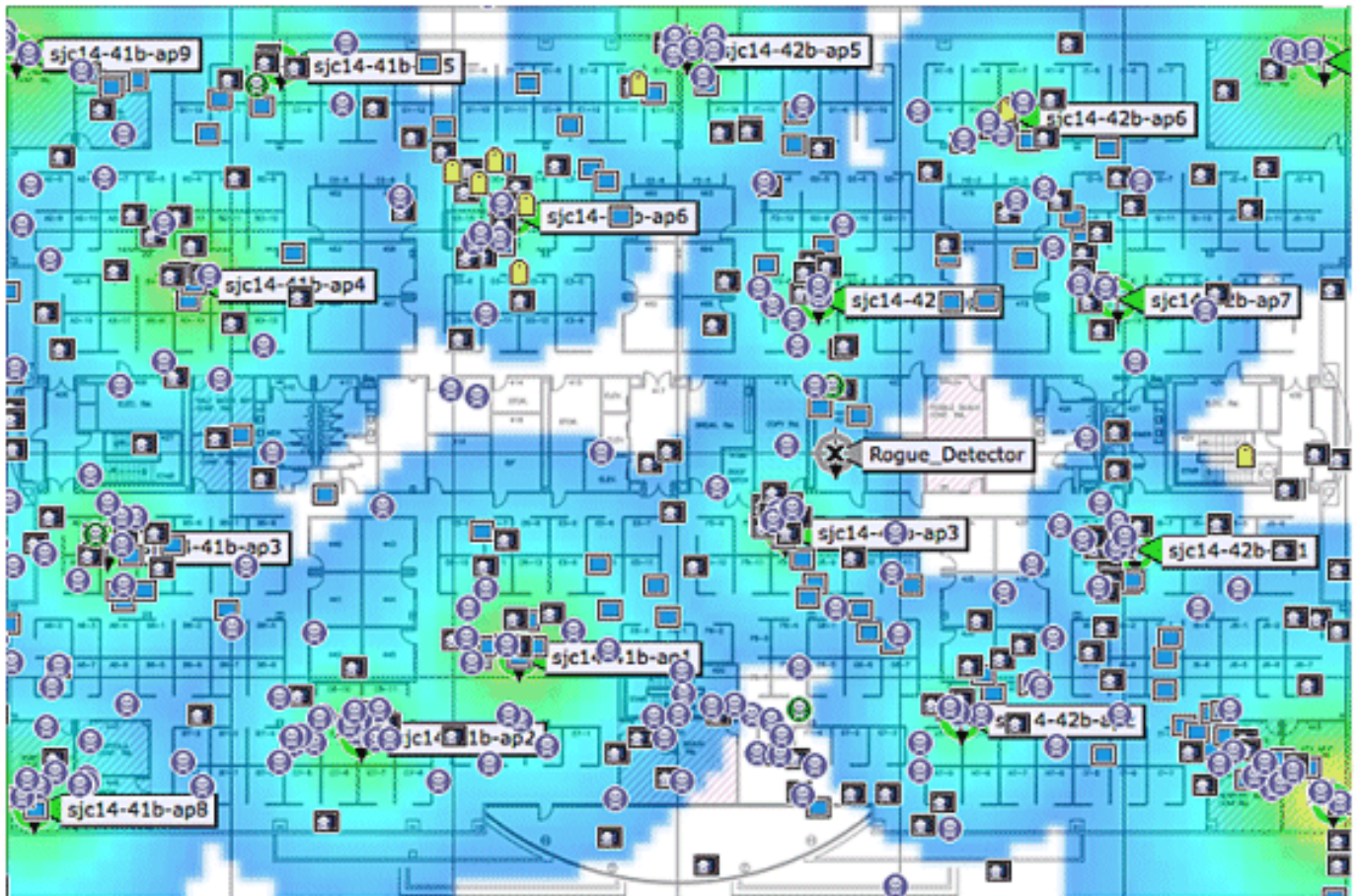
Nicht autorisierter Access Point: Jeder Access Point, der nicht zur Wireless LAN-Mobilitätsgruppe gehört, die ihn erkannt hat. Dies umfasst alle Access Points, die nicht zum System gehören, und zwar innerhalb des Funkbereichs eines Lightweight Access Points. Dazu gehören auch Access Points aus dem kabelgebundenen Netzwerk oder Access Points aus anderen kabelgebundenen Netzwerken (z. B. Access Points eines Nachbarn). Da alle Lightweight Access Points einen Hash als Teil des Beacon-Frames mit einem speziellen Schlüssel verwenden, werden selbst gefälschte Infrastruktur-Access Points als nicht autorisierte Access Points identifiziert und nicht fälschlicherweise als legitime Access Points, die im WCS als Spoof Access Points gekennzeichnet sind.

Nicht autorisierte Clients: Alle Geräte, die nicht autorisierten Access Points zugeordnet sind.

Aktive RFID-Tags: Wi-Fi-Gerät, das erkannt und in einem Wi-Fi-Netzwerk angeordnet werden kann. Auf dem Markt gibt es eine Vielzahl von Wi-Fi-kompatiblen Tags. Tags bieten eine Reihe von Funktionen wie Telemetrie, z. B. Bewegungsdaten und Umgebungsdaten wie Temperatur und Luftfeuchtigkeit, Anrufschaltflächen, Innen- und Außenbetrieb, selbstsichere Versionen und flexible Montageoptionen.


Die MSE ermöglicht die Nachverfolgung von bis zu 18.000 Geräten (Tags, Clients und nicht autorisierte Clients/APs). **Abbildung 1** ist ein Beispiel für eine Bodenkarte, wie im WCS gezeigt, und zeigt Tags, Clients, nicht autorisierte Clients und nicht autorisierte APs an. Die Bodenübersicht zeigt die Skalierbarkeit und Vielfalt der Geräteklassen, die von der MSE nachverfolgt werden können. WCS bietet die Möglichkeit, Suchparameter zu definieren, die nur in einem Teil der Geräte angezeigt werden. So kann beispielsweise ein biomedizinischer Benutzer nur Infusionspumpen und EKG-Maschinen sehen, die mit freundlichen Bezeichnern benannt werden, anstatt unberechtigte Geräte oder Geräte mit kryptischen MAC- oder IP-Adressen.

Abbildung 1: WCS-Bodenübersicht mit verfolgten Geräten



Kunde: 

Tag: 

Nicht autorisierter AP (rot = bössartig, grün = freundlich, grau = nicht klassifiziert) 

Nicht autorisierte Clients: 

Technologie-Hintergrundinformationen

Es gibt zwei Technologien, mit denen Wi-Fi-Geräte mit der Cisco Mobility-Lösung verfolgt werden können:

- RSSI (Signalstärke-Indikation empfangen)
- TDOA (Zeitdifferenz der Ankunft)

Einzelheiten zu diesen Technologien finden Sie im [Designleitfaden für Wi-Fi Location-Based Services 4.1](#).

RSSI (Signalstärke-Indikation empfangen)

RSSI ist die gemessene Leistung eines empfangenen Funksignals. Die Pakete, die von einem Wireless-Gerät übertragen werden, werden an mehreren APs empfangen (vorausgesetzt, dass diese APs den Kanal überwachen, auf dem der Frame übertragen wurde). Die APs leiten diese Pakete zusammen mit den entsprechenden RSSI-Informationen, die am WAP gemessen wurden,

an den WLAN-Controller weiter. Der Wireless LAN Controller aggregiert diese Informationen auf Gerätebasis von verschiedenen APs. Diese Daten werden über NMSP an die MSE weitergeleitet. Die kontextsensitiven Dienste, die sich in der MSE befinden, verwenden die RSSI-Daten, die von einem oder mehreren WLCs empfangen wurden, um den Standort eines Wireless-Geräts zu bestimmen.

RSSI wird in der Regel für Innenräume oder Umgebungen mit niedriger Decke bevorzugt, was zu einer Reflektion der Signale führen kann. Im Gegensatz zu TDOA erfordert RSSI keine exakte Zeitsynchronisierung zwischen APs. Bei den gemessenen RSSI-Werten verschiedener Access Points wird die Wahrscheinlichkeit des Standorts eines Geräts an verschiedenen Stellen im Boden berechnet. Basierend auf dieser Wahrscheinlichkeit wird der Standort als geschätzter Ort zurückgegeben.

[TDOA \(Zeitdifferenz der Ankunft\)](#)

Wenn Sie Tags in Außen- und Außenbereichen verfolgen, wie sie beispielsweise in Umgebungen mit hoher Decke in Innenräumen zu finden sind, ist der Time Different on Arrival (TDOA)-Mechanismus die bevorzugte Methode zur Bestimmung des Gerätestandorts. Bei TDOA wird der Standort eines WLAN-Geräts anhand der Differenz in der Ankunftszeit (TOA) des Signals ermittelt, das es überträgt, wie drei oder mehr zeitsynchronisierte Wi-Fi TDOA-Empfänger erkennen. Die Daten zur Ankunftszeit werden erfasst und an die Context Aware Engine für Tags übermittelt, die sich auf der MSE befinden. Diese berechnet die Zeitunterschiede bei der Ankunft zwischen mehreren Paaren von Wi-Fi-TDOA-Empfängern. Die Zeit, die erforderlich ist, damit eine bestimmte Nachricht von verschiedenen Wi-Fi-TDOA-Empfängern empfangen werden kann, ist proportional zur Länge des Übertragungsweges zwischen dem mobilen Sendegerät und jedem TDOA-Empfänger. Dieser Mechanismus zur Berechnung des Gerätestandorts erfordert die Zeitsynchronisierung zwischen den Wi-Fi-TDOA-Empfängern.

Um eine genaue Position berechnen zu können, sind für diese Methode mindestens drei Wi-Fi-TDOA-Empfänger erforderlich. Die Entfernung zwischen den Wi-Fi TDOA-Empfängern ist relativ größer als die Entfernung zwischen Access Points, die für die RSSI-Positionierung in Innenräumen erforderlich sind. Wie bei der RSSI-Positionierung beruht diese Methode auf unidirektionaler Kommunikation (Tag-Übertragung des Benachrichtigungsrahmens, keine Zuordnung erforderlich).

Weitere Informationen finden Sie im [Konfigurationsleitfaden für kontextsensitive Servicesoftware](#).

[Aktive RFID-Tags](#)

CCX-konforme aktive RFID-Tags werden in einem Wi-Fi-Netzwerk anhand von Tag-Benachrichtigungsrahmen erkannt, die vom Tag gesendet und von einem 802.11-Zugangspunkt empfangen werden. Die Tag-Benachrichtigungs-Frame-Rate kann basierend auf dem jeweiligen Anwendungsfall programmiert werden. In der Regel werden Tags so konfiguriert, dass Tag-Benachrichtigungsrahmen alle 3 bis 5 Minuten übertragen werden, um häufige Standortaktualisierungen und die Akkulaufzeit zu optimieren.

Die Anruftaste-Funktion ermöglicht das Auslösen von Ereignissen auf der Grundlage von Drucktasten auf dem Tag. Dies ermöglicht erweiterte Funktionen wie Notfall-Reporting oder Ersatzteilauffüllung. Einige Tags stellen mehr als eine Anruftaste bereit. Die zweite Anruftaste kann für zusätzliche Funktionen programmiert werden.

Tags können vorprogrammierte Nachrichten speichern, die von der Wireless-Netzwerkinfrastruktur

empfangen werden können. Ein Akku wird zur Stromversorgung aktiver Tags verwendet, die eine Akkulaufzeit von bis zu vier Jahren ermöglichen. Die Akkulaufzeit hängt von einer Reihe von Tag-Konfigurationsparametern ab, darunter die Häufigkeit der Frame-Übertragung von Tagbenachrichtigungen und die Wiederholungsrate. Tags können einen Bericht über den Akkuladestand erstellen und bei niedrigem Akkuladestand Warnmeldungen ausgeben. Tags können auch über einen integrierten Bewegungssensor verfügen, um Tag-Benachrichtigungsrahmen bei Bewegung zu übertragen. Dies trägt dazu bei, die Akkulaufzeit bei stehendem Tag zu erhalten. Konfigurieren Sie die Tags so, dass sie weniger häufig übertragen werden, wenn sie sich nicht bewegen.

Es gibt eine weitere Kategorie von Tags, die erweiterte Sensortechnologie hinzufügen, um den Zustand einer Ressource genau zu überwachen, z. B. ihre Umgebungstemperatur, zusätzlich zu anderen Standort- und Statusinformationen. Diese Sensor-Tags verwenden Standard-Wi-Fi-Netzwerke, um Daten zu den einzelnen Geräten und Sensoren zu übertragen. Es sind keine dedizierten oder proprietären Sensornetzwerke erforderlich.

Wi-Fi-RFID-Tags, die mit der Spezifikation von Cisco Compatible Extensions (CCX) für Wi-Fi-Tags konform sind, können optional Tag-Telemetrieinformationen an das standortbasierte Cisco UWN als Teil der Payload von Tag-Nachrichten weiterleiten. Telemetrieinformationen werden von den Access Points empfangen und von den WLCs erfasst. Beim MSE-Start abonniert die MSE alle Dienste, an denen sie interessiert ist, z. B. die Messwerte für Tags. Der WLC sendet weiterhin die MSE-Benachrichtigungen am Ende jedes Aggregationszyklus.

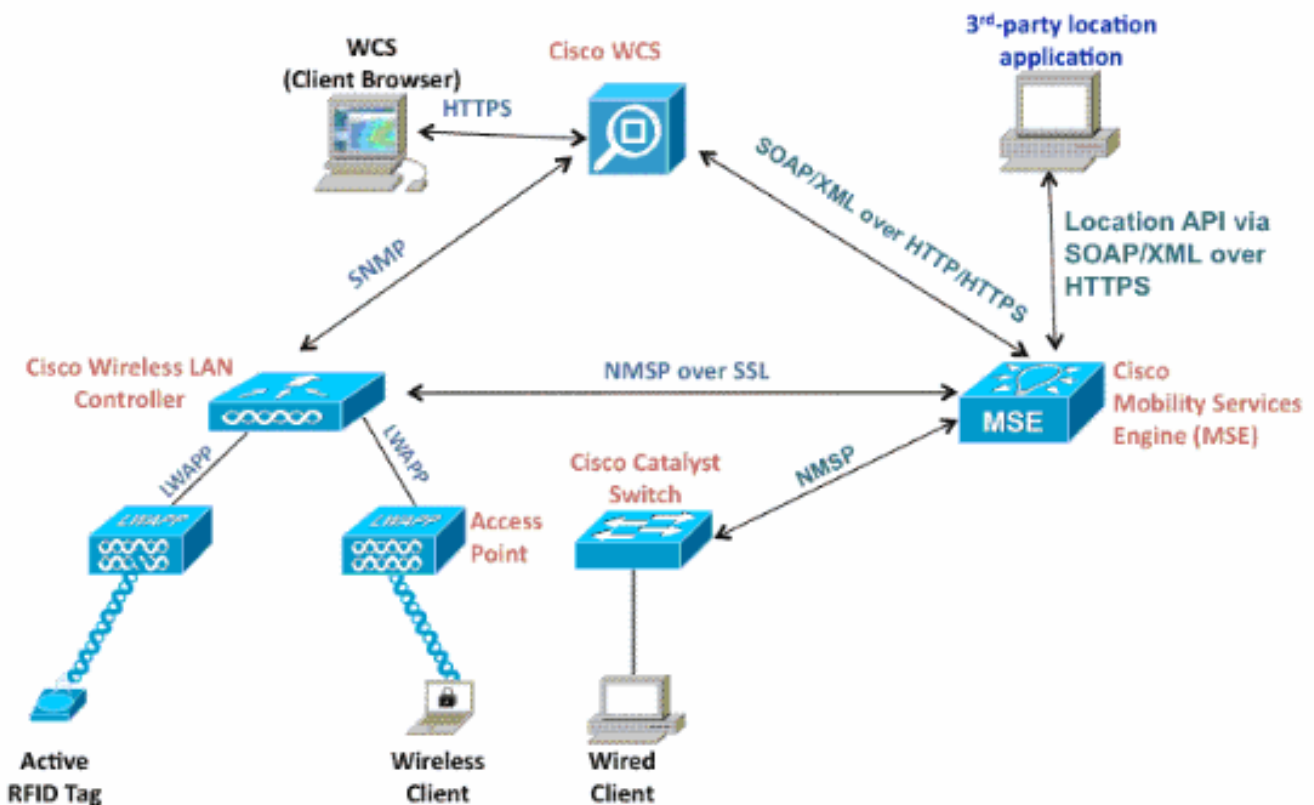
Die Telemetrieinformationen werden von einem CCX-kompatiblen Tag übertragen und von einem oder mehreren APs und/oder Standortempfängern empfangen, d. h. von Wi-Fi TDOA-Empfängern, die die Telemetrieinformationen wiederum an ihre jeweiligen registrierten WLAN-Controller weiterleiten. Wenn die Tags so konfiguriert sind, dass pro Kanal mehrere Frame-Kopien (oder Bursts) gesendet werden, eliminiert der Controller jedes doppelte Tag-Telemetrie und übergibt die destillierten Telemetriewerte an die MSE. Die Datenbank in der MSE wird mit den neuen Telemetrieinformationen aktualisiert und über die SOAP/XML-API für Standortclients verfügbar gemacht.

Bei einem Tag, der den Telemetriewert übergibt, ist NMSP so ausgelegt, dass Telemetriewerte effizient von mehreren Tags übertragen werden können. Der Telemetrie-Datenverkehr von mehreren Tags wird vom WLC aggregiert, wobei jeder NMSP-Endpunkt in der Lage ist, die Fragmentierung und Reassemblierung von NMSP-Frames bei Bedarf durchzuführen. Alle Tag-Daten können in die Northbound-Benachrichtigungen eingeschlossen werden, darunter Telemetrie, Anrufschaltflächen, Chokeypoint-Begegnungen usw.

Systemarchitektur

Die MSE lässt sich wie in **Abbildung 2** gezeigt in die zentralisierte Wireless LAN-Architektur von Cisco integrieren. Die MSE befindet sich außerhalb des Datenpfads des Wireless LAN (siehe Diagramm) und empfängt Daten vom WLC bis zum NMSP. WCS wird zum Konfigurieren der MSE verwendet. Nach der Konfiguration ist die MSE eigenständig.

Abbildung 2: Systemarchitektur



Bei der Bereitstellung der kontextsensitiven Lösung müssen der verfolgte Gerätetyp und die maximale Geräteanzahl berücksichtigt werden. Sie können jeden der fünf Gerätetypen (Wi-Fi-Clients, aktive RFID-Tags, nicht autorisierte Clients, nicht autorisierte APs oder kabelgebundene Clients) einzeln oder zur gleichzeitigen Nachverfolgung konfigurieren.

Eine MSE kann nur von einem WCS verwaltet werden, d. h. eine einzige MSE kann nicht von mehreren WCS-Instanzen verwaltet werden, aber ein einziger WCS kann mehrere MSEs verwalten. Wenn die Anzahl der zu verwaltenden Geräte die Kapazität einer einzelnen MSE übersteigt, müssen mehrere unabhängige MSEs bereitgestellt werden. Die Möglichkeit, mehrere MSEs für die Skalierung bereitzustellen, gilt für alle Dienste, die derzeit auf MSE unterstützt werden. Die maximale Anzahl von Geräten, die von einer Cisco MSE 3350 verfolgt werden können, beträgt 18.000 Geräte (Kombination aus Wi-Fi-Clients, aktiven RFID-Tags, nicht autorisierten Clients, nicht autorisierten APs und kabelgebundenen Clients) im Rahmen des Context Aware Service. Die Cisco MSE 3310 kann bis zu 2.000 Geräte überwachen. Wenn die Anzahl der zu verwaltenden Geräte die Kapazität einer einzelnen MSE-Box übersteigt, müssen mehrere unabhängige MSE-Appliances bereitgestellt werden. Dies kann MSEs auf bestimmten Controllern erfordern, insbesondere auf großen Campus-Umgebungen, in denen das Roaming von Clients oder Ressourcen über verschiedene physische Gebäude oder Domänen erfolgen kann. In diesem Fall können Controller mit maximal 10 MSE-Appliances kommunizieren.

Cisco LAPs arbeiten in einem einzigartigen Dual-Mode, der Geräte sowohl auf den Kanälen erkennt, auf denen sie Clients betreiben, als auch auf allen anderen Kanälen, wenn sie regelmäßig Hintergrundscans durchführen, aber dennoch den Datenzugriff auf ihre Wireless-Clients ermöglichen. Die gesammelten Rohstandortdaten werden dann von jedem Access Point über das LWAPP oder das standardbasierte CAPWAP-Protokoll an den zugehörigen WLC weitergeleitet. Die Daten werden über eine sichere NMSP-Verbindung zwischen dem Wireless LAN-Controller und der MSE übertragen.

Cisco WCS wird zur Verwaltung und Konfiguration der MSE verwendet und kann auch das visuelle Front-End der MSE zur Anzeige nachverfolgter Wi-Fi-Geräte werden. Alle Gerätedetails (kabelgebunden und Wireless) sowie spezifische Verlaufsstandortinformationen können über die

MSE Northbound-API abgerufen werden. WCS verwendet diese Schnittstelle, um Standortinformationen anzuzeigen und kontextsensitive Parameter anzuzeigen und zu konfigurieren.

Die Cisco Mobility-Lösung besteht aus zwei Location Engines mit einer einzigen Unified Application Programming Interface (API):

- Kontextsensitive Engine für Clients (Cisco Engine)
- Kontextsensitive Engine für Tags (Partner-Engine)

Die Context Aware Engine für Clients ist eine RSSI-basierte Lösung und eignet sich ideal zur Verfolgung von Wi-Fi-Client-Geräten in Innenräumen, z. B. Büros, Krankenhäusern oder anderen Umgebungen mit niedriger Decke. Diese Engine wird standardmäßig auf allen Cisco MSE-Servern ausgeliefert. Neben der Cisco MSE müssen Kunden zwei zusätzliche Komponenten für die Client-Verfolgung erwerben:

- Client Tracking-Lizenz für die MSE mit entsprechender Client-Anzahl
- Cisco WCS PLUS mit Standort

Die Context Aware Engine für Tags kann sowohl eine RSSI- als auch eine TDOA-basierte Engine verwenden. Sie ist für die Verfolgung von Wi-Fi-Geräten in Innen-, RSSI-, Innen- und Außenumgebungen (High-Density, TDOA) vorgesehen. Diese Engine wird standardmäßig auch auf allen MSE-Plattformen installiert und ist lizenziert. Kunden müssen diese zusätzlichen Komponenten für die Kundenverfolgung erwerben:

- Tag-Tracking-Lizenz für die MSE mit entsprechender Tag-Anzahl (TDoA oder RSSI)
- Wi-Fi TDoA-Standortempfänger (falls und falls erforderlich)
- LR-Lizenz für jeden Wi-Fi-TDoA-Empfänger
- Cisco WCS PLUS mit Standort

Wenn eine Cisco MSE einem Cisco Unified Wireless Network hinzugefügt wird, übernimmt die MSE die Verantwortung für mehrere wichtige Aufgaben:

- Ausführung von Positionierungsalgorithmen
- Pflege der Kalibrierinformationen
- Auslösung und Versand von Standortbenachrichtigungen
- Verarbeitung von Statistiken und historischem Standort

WCS ist die Verwaltungsplattform für die MSE-Server und als Benutzeroberfläche (user interface, UI) für die Dienste, die die MSE bereitstellt. Der Zugriff auf die MSE erfolgt direkt über SSH oder eine Konsolensitzung zu Wartungs- und Diagnosezwecken. Die gesamte Interaktion zwischen Bediener und Benutzer und der MSE erfolgt in der Regel über WCS.

Die Integration einer Cisco MSE in eine Cisco Unified Wireless Network-Architektur ermöglicht sofort Verbesserungen der Funktionen auf der Basisebene. Enthalten sind folgende Verbesserungen:

Skalierbarkeit: Wenn Sie eine Cisco MSE hinzufügen, erhöht sich die Skalierbarkeit des Cisco UWN von der bedarfsgerechten Nachverfolgung eines einzelnen Geräts zu einer maximalen Nachverfolgungskapazität von bis zu 18.000 Geräten gleichzeitig (WLAN-Clients, RFID-Tags, nicht autorisierte Access Points und nicht autorisierte Clients) pro MSE. Bei Bereitstellungen, die die Unterstützung einer größeren Anzahl von Geräten erfordern, können zusätzliche MSE-Appliances unter einem oder mehreren WCS-Servern bereitgestellt und verwaltet werden.

Verlaufs- und Statistiktrends - Die MSE zeichnet Verlaufs- und Statistikinformationen für Clients

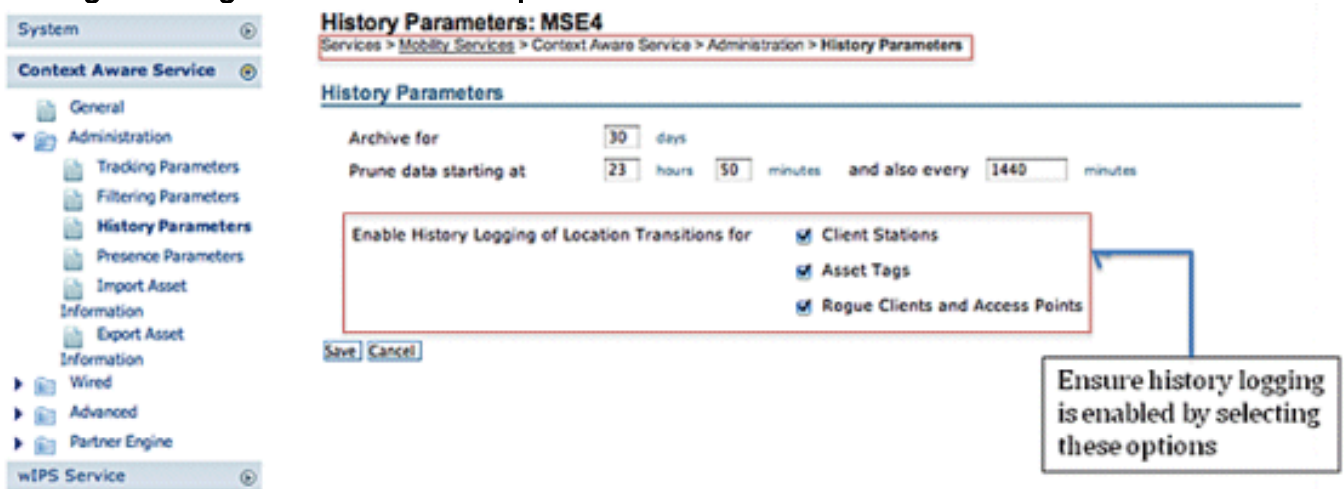
und Tags auf und verwaltet diese. Diese Informationen können über WCS oder mit Standortsystemen von Drittanbietern angezeigt werden. Diese Verlaufsdaten können für Standorttrends, Untersuchungen von Ressourcenverlusten, das Management von RF-Kapazitäten und die Erleichterung der Behebung von Netzwerkproblemen verwendet werden.

Verlaufparameter können in WCS konfiguriert werden, wie in **Abbildung 3** gezeigt.

Es gibt mehrere Variablen, die sich auf die Menge der Verlaufsdaten auswirken, die auf der MSE gespeichert werden können: durchschnittliche Anzahl beweglicher Elemente, durchschnittliche zurückgelegte Entfernung bei jeder Bewegung, Informationsübergänge, Telemetrieinformationen von Tags usw.

Standardmäßig werden in der MSE 30 Tage Verlaufsdaten gespeichert.

Abbildung 3: Konfigurieren der Verlaufparameter



Dies sind wichtige Punkte zum Standortverlauf:

1. Die Verlaufsverfolgung muss aktiviert sein (wie gezeigt), um Verlaufsdaten über ein Element abzurufen.
2. Die Anzahl der Tage der Verlaufsgeschichte und der Beschneidungszeit muss korrekt festgelegt werden (siehe Screenshot).
3. Obwohl die Anzahl der Tage, in denen der Verlauf gespeichert werden soll, nicht auf der Benutzeroberfläche beschränkt ist, ist die auf dem Server gespeicherte Historie durch den Speicherplatz und die Auswirkungen auf die Leistung auf das Gesamtsystem begrenzt.
4. Der Verlauf eines Elements wird nur aufgezeichnet, wenn diese auftreten: Er bewegt sich über 10 m oder 30 Fuß. Wenn die Notfall- oder Paniktaste auf den Tags gedrückt wird. Wenn das Tag an einem Erreger vorbeigeht. Wenn sich der Boden ändert, d. h., das Element bewegt sich zwischen den Etagen.
5. Ein Element wird als "inaktiv" deklariert, wenn es eine Stunde lang inaktiv bleibt. Wenn sie 24 Stunden lang inaktiv bleibt, wird sie aus der Verfolgungstabelle entfernt. Wenn das Element aus der Verfolgungstabelle entfernt wurde, ist es nicht möglich, die historische Position des Elements auf der WCS-Überwachungsseite zu sehen, obwohl der Verlauf des Elements 30 Tage lang in der MSE noch vorhanden ist. Der fehlende Eintrag für das Datenbereinigungsintervall (siehe **Abbildung 4: Standortparameter**) erleichtert die Steuerung der Verfolgungstabelle.

Location Parameters: MSEWCS4

Services > Mobility Services > Context Aware Service > Advanced > Location Parameters

Location Parameters

Enable calculation time	<input type="checkbox"/>	Enable
Enable OW Location	<input type="checkbox"/>	Enable
Relative discard RSSI time	<input type="text" value="3"/>	1 - 99999 min
Absolute discard RSSI time	<input type="text" value="60"/>	1 - 99999 min
RSSI Cutoff	<input type="text" value="-75"/>	-90 to -50 dBm
Enable Location Filtering	<input checked="" type="checkbox"/>	Enable
Chokepoint Usage	<input checked="" type="checkbox"/>	Enable
Use Chokepoints for Interfloor conflicts	<input type="text" value="Never"/>	
Chokepoint Out of Range Timeout	<input type="text" value="60"/>	1-99999 secs
Absent Data cleanup interval	<input type="text" value="1440"/>	1 - 99999 mins

Wenn jeder Übergang als Speicherereignis in der historischen Datenbank protokolliert und die Tabelle "Location History" (Standortverlauf) aus Leistungsgründen auf 10 Millionen Zeilen begrenzt wird, wird in **Tabelle 1** die Anzahl der Tage zusammengefasst, die erforderlich sind, um diesen Grenzwert zu erreichen. Je größer die Anzahl der Elementübergänge pro Minute ist, desto größer ist der belegte Speicherplatz. Laut Tabelle dauert es nur 7,14 Tage, 10 Millionen Zeilen mit 1000 Übergängen/Minute zu erreichen. Mit der Standardeinstellung von 30 Tagen Verlaufsdaten verbrauchen 1000 Übergänge/Minute übermäßig viel Speicherplatz, da MSE Verlaufsdaten nicht löscht, bevor das 30-Tage-Fenster erreicht wurde.

Cisco empfiehlt, den Verlaufparameter für Geräte, die häufig auf einen Wert von weniger als 30 Tagen verschoben werden, zu ändern.

Tabelle 1: Datenbank-Limit für Standortversionsverlauf

Übergänge pro Minute	Tage bis zum Erreichen von 10 Millionen Zeilen
100	69.44
200	34.72
300	23.15
400	17.36
500	13.89
600	11.57
700	9.92
800	8.68

900	7.75
1000	7.14

Chokepoint Location - Die MSE bietet eine präzise und deterministische Lokalisierung, basierend auf der Übertragung eines Anlageguts durch einen beschränkten physischen Bereich, der als Treffpunkt bezeichnet wird. Chokepoint-Trigger (auch als "Exziter" bezeichnet) in diesen Bereichen und in der Nähe von getaggten Ressourcen stimulieren die Tags mit Niederfrequenz-Signalisierung (125 kHz). Die RFID-Tags übertragen dann die Identität des Chokepoint-Triggers an die Cisco UWN-Infrastruktur. Die im Tag-Paket enthaltenen Chokepoint-Informationen liefern der MSE Informationen zum Überschreiben von RF-Fingerprinting-Standortkoordinaten und zum Übernehmen der Checkpoint-Position für eine bestimmte Dauer. Die Genauigkeit der Näherungslage kann je nach Funktion des Chokepoint-Triggers zwischen einem Radius von unter einem Fuß und über 25 Fuß (25 bis 650 cm) liegen. Anwendungen für den Chokepoint-Standort reichen von allgemeinen Verwendungszwecken wie Diebstahlschutz für wertvolle Ressourcen bis hin zu branchenspezifischen Prozesssteuerungsereignissen, wie sie beispielsweise in Fertigungsbetrieben verwendet werden.

Cisco Extensions for Wi-Fi Tags Telemetrie-Informationen und Notfallbenachrichtigungen - Cisco hat in Zusammenarbeit mit einer Vielzahl von Asset-Tag-Anbietern eine erweiterbare Spezifikation für 802.11 Wi-Fi-basierte aktive Asset-Tags erstellt. Die Cisco Compatible Extensions (CCX)-Wi-Fi-Tag-Spezifikation definiert ein gemeinsames Übertragungsformat, das Tag-Anbieter für die Zusammenarbeit mit dem kontextsensitiven Cisco UWN verwenden können. Dazu gehört ein grundlegendes Feature-Set, das Telemetrie, Tags für den Leistungsgrad der Übertragung, Akkuinformationen und erweiterte Felder für Notfallgruppen und Checkpoints umfasst. Durch die Ergänzung einer MSE können Kunden diese Funktionen nutzen und von den Vorteilen profitieren, die sich durch die Möglichkeit ergeben, im selben Netzwerk konforme Asset-Tags verschiedener Anbieter "zusammenzufügen". Derzeit haben Tag-Anbieter CCXv1 implementiert. Tag-Referenz-URL: http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html

[Abschnitt 2: Planung und Einrichtung Ihres kontextsensitiven Netzwerks](#)

Bei der Bereitstellung eines Wireless-Netzwerks müssen verschiedene Richtlinien befolgt werden, die sich direkt auf die Genauigkeit des Standorts auswirken.

Entwerfen des Wireless LAN für Standort und Sprache

Allgemeine Richtlinien - RSSI

Um den optimalen Standort aller Geräte in den WLAN-Abdeckungsbereichen zu ermitteln, sollten die Dichte und Platzierung der Access Points berücksichtigt werden.

[Positionierung des Access Points](#)

Die korrekte Platzierung von Access Points oder besser, die Platzierung und der Antennentyp sind einige bewährte Verfahren, die eingehalten werden müssen, um eine angemessene Standortgenauigkeit zu erreichen. In vielen Büro-WLANs sind Access Points hauptsächlich über Innenbereiche verteilt und bieten Services für die umliegenden Arbeitsbereiche. Diese Access Point-Standorte wurden in der Regel anhand der folgenden Abdeckungsstufen ausgewählt: WLAN-Bandbreite, Wiederverwendung von Kanälen, überlappende Zellen, Sicherheit, Ästhetik

und Durchführbarkeit der Bereitstellung. In einem standortbezogenen WLAN-Design müssen die Anforderungen der zugrunde liegenden Daten- und Sprachanwendungen mit den Anforderungen für eine gute Standorttreue kombiniert werden. Je nach Standort sind die Anforderungen des standortbasierten Cisco UWN flexibel genug, um die Standortverfolgung zu Sprachinstallationen hinzuzufügen, die bereits gemäß den Best Practices von Cisco entwickelt wurden. So ist beispielsweise eine umfassende Nachbearbeitung nicht erforderlich. Vielmehr kann die Infrastruktur, die bereits gemäß bewährten Verfahren für Sprachkommunikation bereitgestellt wurde, häufig erweitert werden, sodass die Anforderungen an die Standortverfolgung (z. B. Platzierung des Perimeters und der Eckpunkte der Access Points) je nach den Merkmalen der betroffenen Bereiche ebenfalls erfüllt werden.

Bei einem standortorientierten Design ist es wichtig, sicherzustellen, dass Access Points nicht nur im Inneren und in der Fußbodenmitte angeordnet sind. Die Access Points am Perimeter ergänzen vielmehr die Access Points, die sich innerhalb der Innenbereiche der Etage befinden. Darüber hinaus müssen Access Points in jeder der vier Ecken des Stockwerks und an allen anderen Ecken des Bodenperimeters platziert werden. Diese Access Points am Perimeter spielen eine entscheidende Rolle, um eine gute Standorttreue in den umgebenden Bereichen zu gewährleisten, und können in einigen Fällen auch eine allgemeine Sprach- oder Datenabdeckung bieten.

Wenn Sie den Chokepoint-Standort verwenden, stellen Sie sicher, dass alle für die Installation des Chokepoint-Triggers vorgesehenen Bereiche eindeutig innerhalb des Funkbereichs Ihrer Access Points liegen. Anders als bei passiven RFID-Scannern wird das WLAN verwendet, um die aufregenden Inhalte an die Infrastruktur zu übertragen. Neben der Zusicherung, dass Nachrichten, die über Asset-Tags in Chokepunktbereichen übertragen werden, ordnungsgemäß vom System empfangen werden, kann eine ordnungsgemäße Planung sicherstellen, dass Asset-Tags mit RF-Fingerprinting nachverfolgt werden können, wenn diese sich den Checkpoints nähern und sie verlassen. Die Möglichkeit, Asset-Tags mit RF-Fingerprinting zu verfolgen, ergänzt die Fähigkeit des Systems, getaggte Ressourcen innerhalb von Chokepunktbereichen mit präzisen Chokepoint-Standortstechniken zu lokalisieren.

Die Access Points, die den Perimeter und die Ecken des Bodens bilden, können als eine Gliederung des konvexen Rumpfes oder einer Reihe möglicher Gerätestandorte betrachtet werden, an denen das beste Potenzial für hohe Genauigkeit und Präzision besteht. Der Innenbereich (Innenbereich des konvexen Rumpfes) kann als mit hohem Potenzial für eine gute Standortgenauigkeit angesehen werden. Wenn die verfolgten Geräte in den Bereich außerhalb des konvexen Rumpfes streuen, verschlechtert sich die Genauigkeit.

Um eine geeignete konvexe Rumpf-Einrichtung rund um die Standortzentren sicherzustellen, die ein hohes Präzisionspotenzial aufweisen, müssen Access Points in jeder Etage des Bodens sowie am Bodenperimeter zwischen Ecken platziert werden. Die Trennung der Access Points entlang des Perimeters muss den allgemeinen Richtlinien für die Trennung der Access Points (wie in einem nachfolgenden Abschnitt beschrieben) entsprechen. Der Designer kann diesen Abstand ggf. reduzieren, damit diese Access Points Sprach- oder Datendienste für den Boden bereitstellen können.

Stellen Sie sicher, dass nicht weniger als drei Access Points für jeden Bereich zuständig sind, in dem der Gerätestandort erforderlich ist. Für optimale Genauigkeit sind vier oder mehr APs erforderlich. Dadurch wird auch das Risiko verringert, dass APs aufgrund anderer WLAN-Aktivitäten nicht immer zum Standort beitragen. In einer normalen Büroumgebung müssen die Access Points den Standort aller nachverfolgten Wi-Fi-Geräte umgeben. Ein Access Point muss alle 40 bis 70 Fuß (~12 bis 20 Meter) positioniert werden. Dies bedeutet, dass alle 2.500 bis 5.000 Quadratmeter (~230-450 Quadratmeter) ein Access Point vorhanden ist. So sind beispielsweise in

einer Einrichtung mit einer Fläche von 200.000 m² 40 APs (200.000/5.000) erforderlich, um eine angemessene Wi-Fi-Abdeckung zu gewährleisten. AP-Antennen müssen in einer Höhe von mindestens 3 m und einer Höhe von maximal 6 m platziert werden. Da diese Richtlinien stark von der Bauweise und den verwendeten Materialien abhängen, müssen andere Faktoren und Empfehlungen berücksichtigt werden. In der Regel muss für die Geräteverfolgung von mindestens drei APs im gleichen Stockwerk ein Mindestsignalwert von -75 dBm verwendet werden.

Wenn Sie diese Richtlinien befolgen, ist es wahrscheinlicher, dass Access Points nachverfolgte Geräte erfolgreich erkennen.

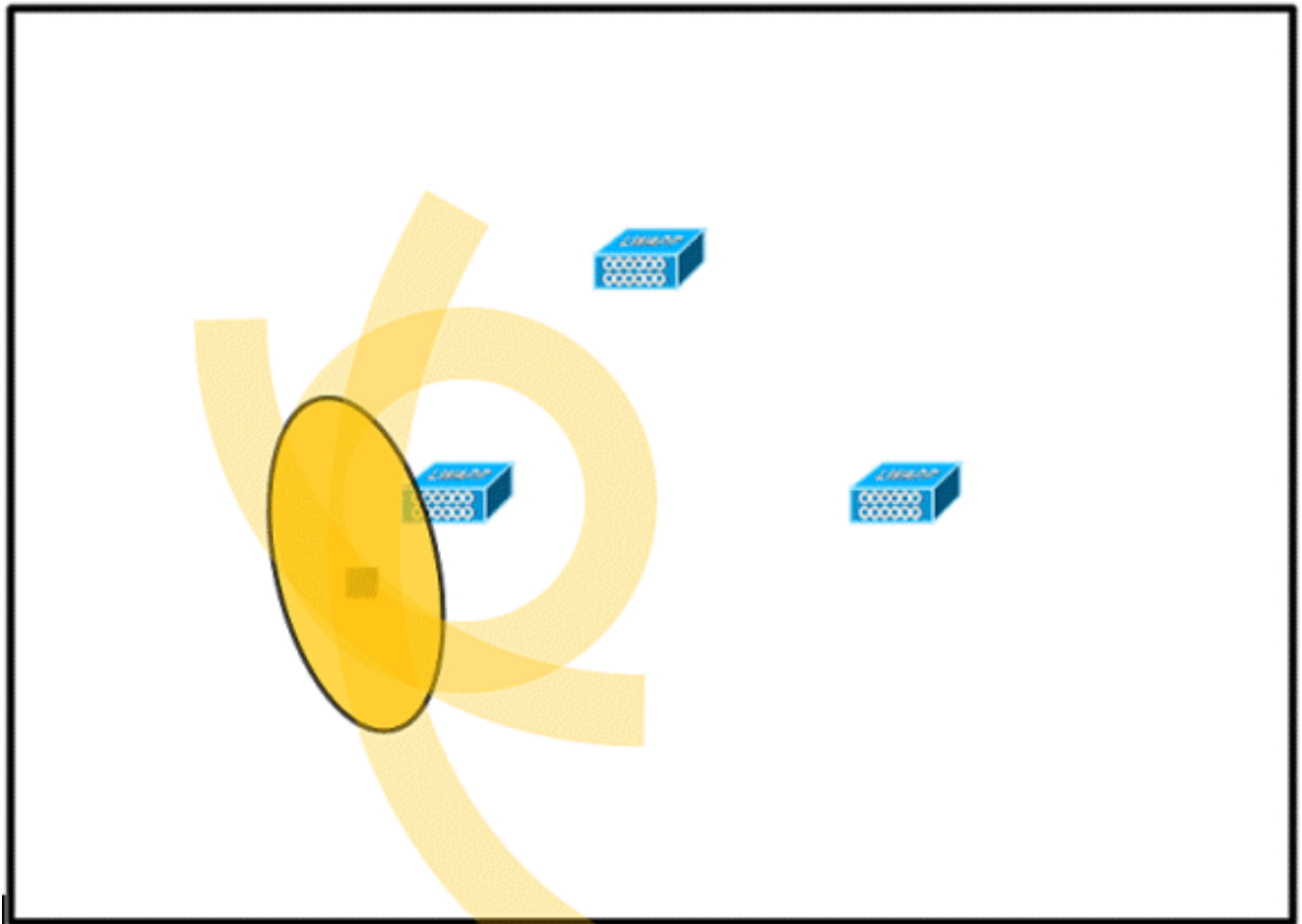
Selten haben zwei physische Umgebungen dieselben Funkeigenschaften. Die Benutzer müssen diese Parameter an ihre spezifische Umgebung und ihre Anforderungen anpassen.

Dies sind die grundlegenden Regeln für die Platzierung von Access Points, die zur Standortgenauigkeit beitragen:

1. Ermöglichen Sie die Abdeckung des AP-Perimeters.
2. Sorgen Sie für eine ausreichende AP-Dichte.
3. Verstärkte APs, insbesondere in Gebieten mit langer und enger Abdeckung.
4. Entwerfen Sie ein Wireless-Netzwerk für alle Anwendungen (Daten, Sprache und Standort).
5. Überprüfung der Wireless-Bereitstellung mithilfe einer Standortuntersuchung
6. In einem Gebäude mit ähnlich geformten Etagen stellen Sie die Access Points auf jeder Etage in einem ähnlichen Muster bereit. Dadurch wird die Leistung der Bodenseparierung des Systems verbessert.

Mit dem WCS Planning Tool können die korrekte Platzierung und Dichte der Access Points ermittelt/überprüft werden.

1. Positionieren Sie Access Points entlang der Peripherie und in den Ecken der Abdeckungsbereiche, um Geräte in der Nähe von Räumen und Gebäuden zu lokalisieren. Access Points, die in der Mitte dieser Abdeckungsbereiche angeordnet sind, liefern gute Daten über Geräte, die ansonsten in gleicher Entfernung von allen anderen Access Points angezeigt werden (siehe **Abbildungen 5 bis 8**). **Abbildung 5: Kombinierte Access Points können zu schlechten Standortergebnissen führen**



AP:

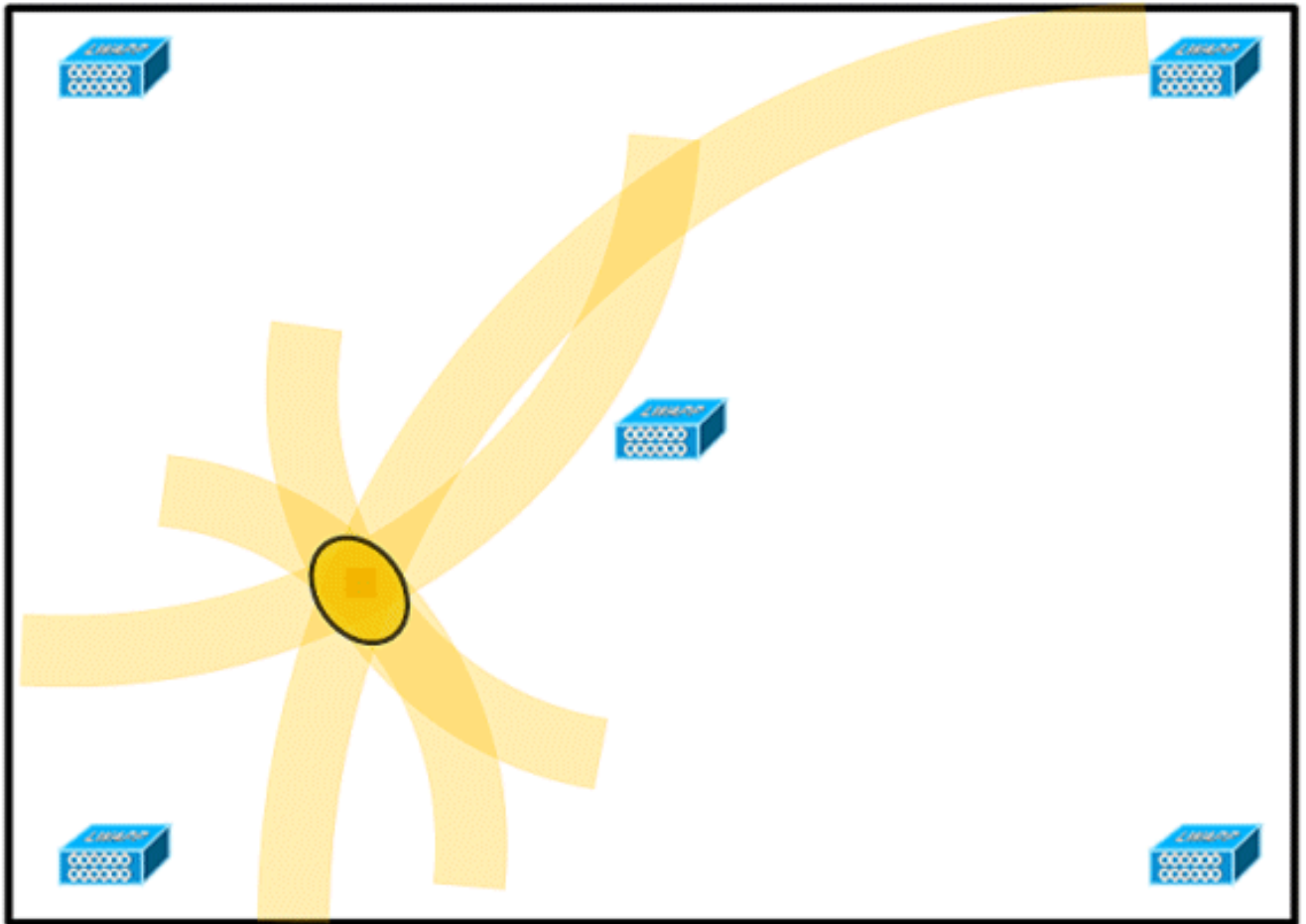
Wi-Fi-Gerät:



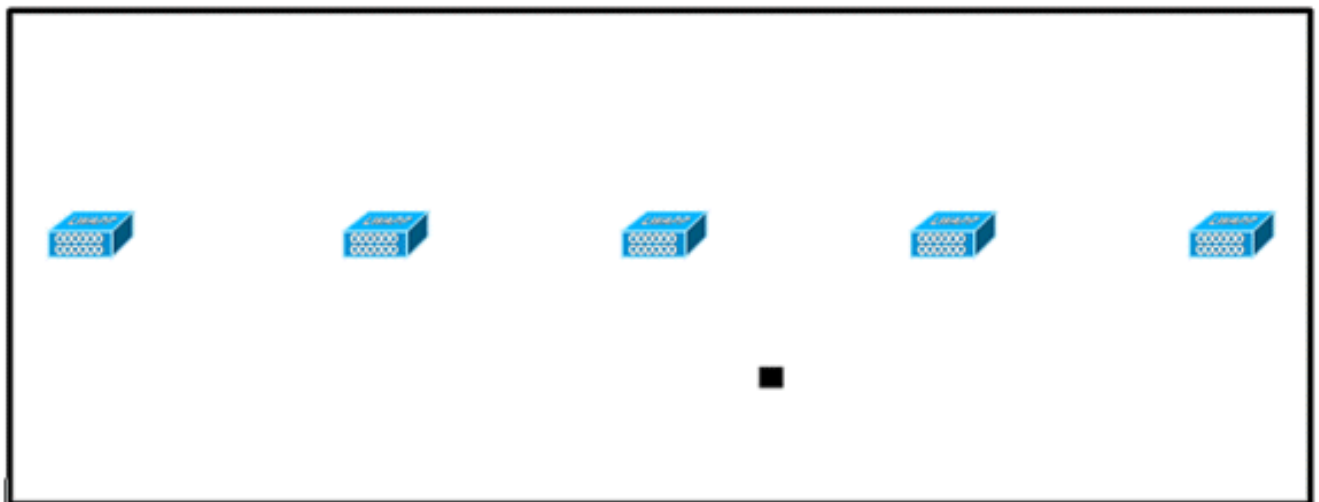
RF-Jitter (möglicher Standort):



2. Erhöhen Sie die Gesamtdichte der Access Points, und verschieben Sie die Access Points zum Perimeter des Abdeckungsbereichs, um die Standortgenauigkeit erheblich zu verbessern (siehe Abbildung). **Abbildung 6: Verbesserte Standortgenauigkeit durch korrekte AP-Platzierung**

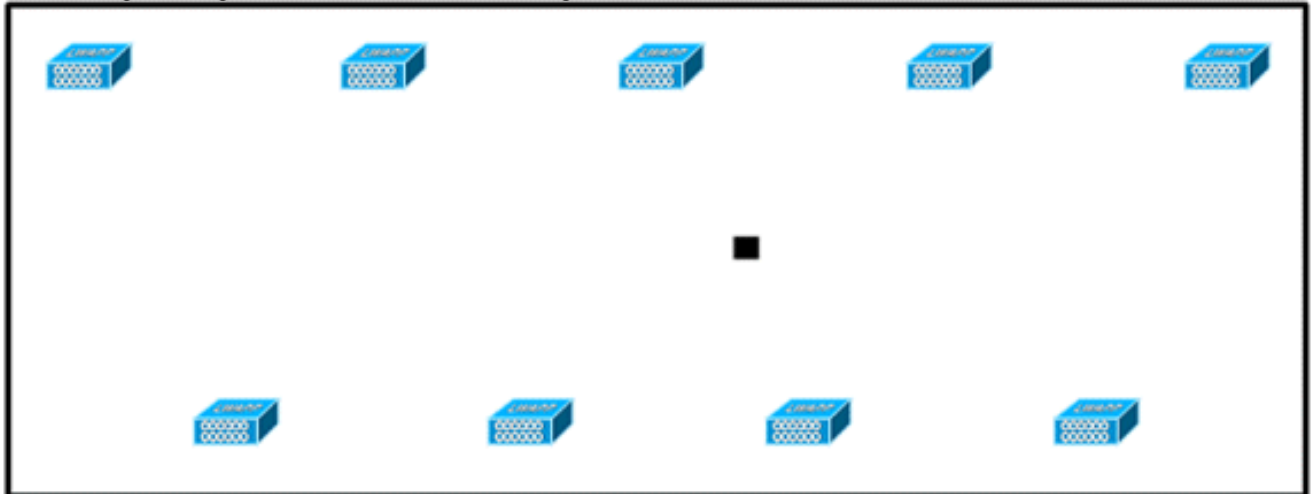


3. Platzieren Sie in Bereichen mit langer und schmaler Abdeckung Access Points nicht gerade (siehe **Abbildungen 7 und 8**). Eine empfohlene Bereitstellung besteht in der Stagnation von APs, da diese eine eindeutige RF-Signatur für jeden Punkt auf der Wi-Fi-Abdeckungsübersicht bereitstellen. Eine geradlinige Bereitstellung bietet eine HF-Karte wie bei einem Mirror-Server. Bei dieser Art der Bereitstellung ähnelt die RF-Signatur eines Punktes in der oberen Seite der Karte der RF-Signatur am Spiegelungspunkt auf der unteren Seite der Karte. **Abbildung 7: Vermeiden Sie die Bereitstellung von APs in einer geraden Linie.**

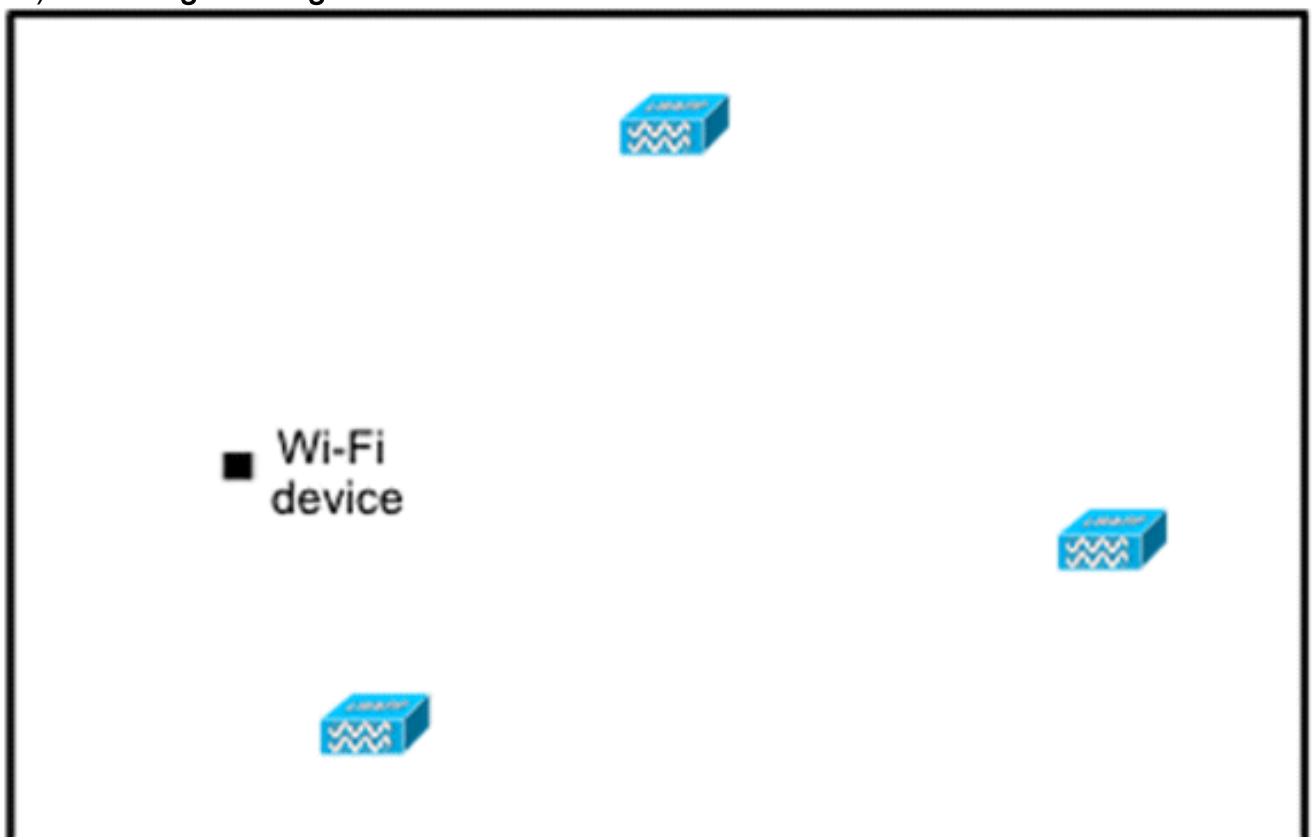


Obwohl das Design in **Abbildung 7** genügend Access Point-Dichte für Anwendungen mit hoher Bandbreite bieten kann, leidet der Standort, da die Ansicht eines einzelnen Geräts für jeden Access Point nicht unterschiedlich genug ist, sodass der Standort des Geräts schwer zu bestimmen ist. Verschieben Sie die Access Points in den Perimeter des Abdeckungsbereichs, und staffeln Sie sie. Jedes Gerät bietet eine deutlich andere Ansicht,

was zu einer höheren Standorttreue führt (siehe **Abbildung 8**). **Abbildung 8: Verbesserte Standortgenauigkeit durch die Verteilung von Access Points rund um den Perimeter**



4. Wenn Sie ein Wireless LAN für eine kontextsensitive Mobilitätslösung entwerfen und gleichzeitig auch Sprachanwendungen planen, müssen Sie eine Reihe von Designfaktoren berücksichtigen. Die meisten aktuellen Wireless-Mobilgeräte unterstützen nur 802.11b, das nur drei überlappungsfreie Kanäle bietet. WLANs für Telefonie sind daher tendenziell weniger dicht als die für die Übertragung von Daten vorgesehenen. Wenn Datenverkehr in der Platinum QoS-Gruppe in die Warteschlange gestellt wird (in der Regel für Sprache und anderen latenzempfindlichen Datenverkehr reserviert), verschieben Lightweight Access Points ihre Scanfunktionen, die es ihnen ermöglichen, auf anderen Kanälen einen Spitzenwert zu erzielen und u. a. Informationen zum Gerätestandort zu sammeln. Daher kann der Benutzer die WLAN-Bereitstellung durch Access Points, die auf den Modus "Monitor Only" (Nur Überwachung) eingestellt sind, ergänzen. Access Points, die nur überwacht werden, bieten Clients keinen Service und verursachen keine Interferenzen. Sie scannen einfach die Funkwellen nach Geräteinformationen (siehe **Abbildungen 9 und 10**). **Abbildung 9: weniger dichte Wireless LAN-Installationen**



WLAN-Installationen mit weniger hoher Dichte, z. B. solche von Sprachnetzwerken, finden eine deutlich höhere Standorttreue, da Access Points mit dem Standort Optimized Monitor Mode hinzugefügt und korrekt platziert werden.

5. Überprüfen Sie die Abdeckung mit einem Wireless-Laptop, einem Handheld und möglicherweise einem Telefon, um sicherzustellen, dass nicht weniger als drei Access Points vom Gerät erkannt werden. Stellen Sie zur Überprüfung der Client- und Ressourcen-Tag-Position sicher, dass das WCS Client-Geräte und -Tags im angegebenen Genauigkeitsbereich meldet (10 m, 90 %). Um diese Genauigkeit zu erreichen, kann eine Kalibrierung erforderlich sein.

Tracking Optimized Monitor Mode (TOMM)

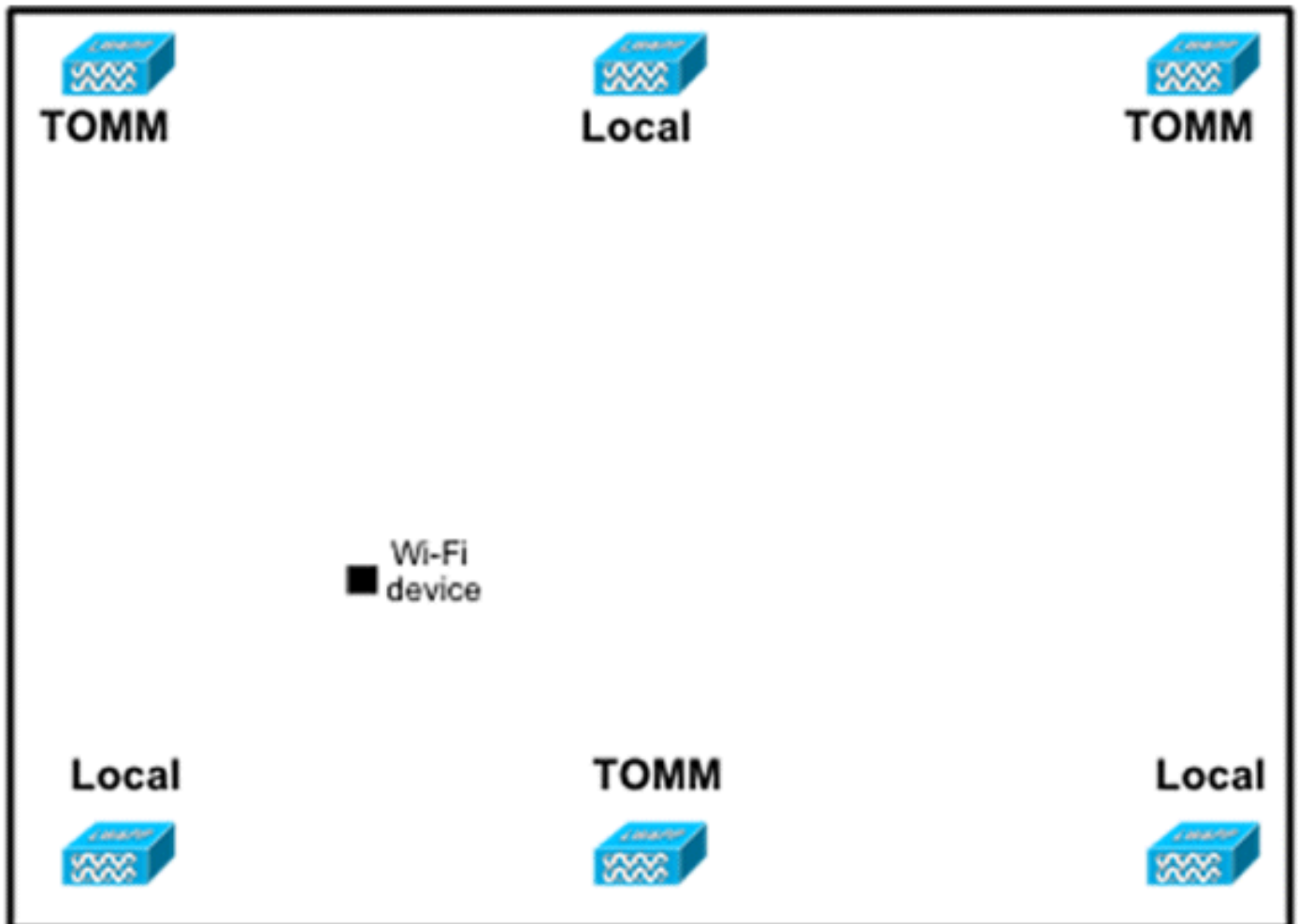
Ab der Softwareversion 5.0 können Cisco Aironet 1100- und 1200-APs als APs für den Überwachungsmodus fungieren. Diese Funktion kann aus folgenden Gründen verwendet werden:

- Standort- und Sprachkommunikation: Bei einer gemischten Bereitstellung des Access Points im Überwachungsmodus ergeben sich keine negativen Auswirkungen auf die Sprachkommunikation, da der Standort eine Erhöhung der AP-Dichte erfordert.
- Low-Touch hat keine Auswirkungen auf die aktuelle Infrastruktur.

Der optimierte Überwachungsmodus für die Nachverfolgung kann verwendet werden, wenn Sie Clients und/oder Tags verfolgen.

TOMM-APs können die Abdeckung für Orte, an denen Wi-Fi-Abdeckung besteht, verbessern, unabhängig davon, wo sie vorhanden sind, entweder am Perimeter oder innerhalb des konvexen Rumpfes. TOMM-APs stören nicht den AP-Betrieb im lokalen Modus. Um die Überwachung und die Standortberechnung von Tags zu optimieren, kann TOMM auf bis zu vier Kanälen im 2,4-GHz-Band (802.11b/g-Funkmodul) eines Access Points aktiviert werden. Dadurch können Channel-Scans nur auf die Kanäle fokussiert werden, auf denen Tags normalerweise für den Betrieb programmiert sind (z. B. Kanäle 1, 6 und 11).

Abbildung 10: Tracking Optimized Monitor Mode AP-Bereitstellung



Platzierung von APs und Antennen

Die Positionierung von APs und externen Antennen kann sich erheblich auf die Leistung des Wireless-Netzwerks auswirken. Dies gilt für die Daten- und Sprachübertragung sowie für die Standortverfolgung. APs und Antennen dürfen nicht an Orten aufgestellt werden (z. B. in der Nähe von I-Strahlen), an denen Signalmuster verzerrt werden können. Ein RF-Null-Punkt wird durch Überquerung von Signalwellen erzeugt, und eine Multi-Path-Verzerrung wird erzeugt, wenn RF-Signale reflektiert werden. Diese Anordnung führt zu einer sehr geringen Abdeckung hinter dem Access Point und einer geringeren Signalqualität vor dem Access Point. Ein I-Strahl erzeugt viele Reflexionen für empfangene und übertragene Pakete. Die reflektierten Signale führen aufgrund von Nullpunkten und Multipath-Interferenzen zu einer sehr schlechten Signalqualität, aber die Signalstärke kann hoch sein, da die AP-Antennen so nahe am I-Strahl liegen, dass sie das Signal verstärken können. Stattdessen müssen der Access Point und die Antennenplatzierung von den I-Strahlen entfernt positioniert werden, sodass weniger reflektierte Signale, weniger Null-Punkte und weniger Multipath-Interferenzen vorhanden sind. Das Prinzip gilt auch für die Platzierung von APs und Antennen in oder in der Nähe der Decke in einer Standard-Unternehmensumgebung. Wenn es Metallluftkanäle, Höhenschächte oder andere physische Barrieren gibt, die eine Signalreflexion oder Multipath-Interferenz verursachen können, empfiehlt Cisco, Antennen von diesen Objekten zu entfernen. Bei großen metallischen Objekten, wie z. B. Aufzüge und Luftkanäle, die Antenne einige Meter entfernt bewegen. Dadurch werden Signalreflexion und -verzerrung eliminiert. **Die Abbildungen 11 bis 13** zeigen eine schlechte Positionierung der Access Points.

Abbildung 11: Schlechte Platzierung des Access Points in der Nähe physischer Hindernisse



Abbildung 12: Schlechte Platzierung des Access Points in der Nähe physischer Hindernisse



Abbildung 13: Schlechte AP-Positionierung - APs dicht nebeneinander aufgestellt



Wenn Sie Access Points mit internen oder externen Antennen installieren, müssen sowohl die Positionierung des Access Points als auch die Ausrichtung der Access Point-Antennen im WCS mit der tatsächlichen Platzierung des Access Points und der Antennenausrichtung übereinstimmen. Dies gewährleistet Genauigkeit und Präzision sowohl bei der Standortverfolgung als auch bei der Darstellung von prädiktiven Wärmebildern. Der Antennentyp, die Positionierung, die Ausrichtung und die Höhe vom Boden aus sind für eine gute Genauigkeit von entscheidender Bedeutung. Wenn Sie die APs in WCS platzieren, stellen Sie sicher, dass die Antennenausrichtung und der Antennentyp mit den bereitgestellten APs übereinstimmen.

Hinweis: Wenn Sie Wireless-Clients überwachen, werden nur Cisco Antennen offiziell unterstützt. Für Antennen von Drittanbietern werden im WCS keine Heatmaps generiert. Dies bedeutet auch, dass RSSI-Werte, die von diesen Antennen empfangen wurden, bei der Standortberechnung ignoriert werden. Für die Tag-Nachverfolgung können sowohl Cisco Antennen als auch Antennen von Drittanbietern verwendet werden.

Der typische Cisco Aironet Access Point ist mit Antennenvielfalt installiert. Antennenvielfalt sorgt für optimale Reichweite und optimalen Durchsatz in Umgebungen mit hohen Multipfaden. Es wird empfohlen, die Antennenvielfalt immer zu aktivieren. Das kontextsensitive Cisco UWN wurde entwickelt, um RSSI-Informationen von beiden Access Point-Antennen bei der Lokalisierung von verfolgten Geräten zu berücksichtigen. Stellen Sie für eine gute Genauigkeit sicher, dass die Antennen an allen Antennenanschlüssen des aktivierten Access Points physisch vorhanden sind. Andernfalls können unregelmäßige RSSI-Messwerte an aktivierten Antennenanschlüssen gemeldet werden, an denen keine angeschlossene Antenne vorhanden ist. Die ungewöhnlich niedrigen RSSI-Werte von Antennenanschlüssen ohne Antennen führen zu einer schlechten Standortgenauigkeit.

Die Wahl der Antenne für die Verwendung mit einem Access Point ist für die Eigenschaften jeder drahtlosen Netzwerkbereitstellung von entscheidender Bedeutung. Im Wesentlichen gibt es zwei Arten von Antennen: direktional und omnidirektional. Jeder Antennentyp ist für eine bestimmte Verwendung geeignet und eignet sich besser für eine bestimmte Art der Bereitstellung. Da Antennen Funksignale in großen, durch Antennendesign bestimmten Empfangsbereichen verteilen, ist die erfolgreiche Abdeckung in hohem Maße von der Antennenauswahl abhängig.

Eine Antenne hat drei grundlegende Eigenschaften: Gewinn, Direktivität und Polarisierung.

- **Gewinn:** Ein Maß für die Erhöhung der Leistung. Gewinn ist die Menge an Energie, die eine Antenne zu einem HF-Signal hinzufügt. Alle Antennen sind passive Elemente. Eine Antenne wird nicht mit Strom versorgt, sondern neu verteilt, um in einer bestimmten Richtung mehr Strahlleistung bereitzustellen als durch eine Rundstrahlantenne (isotrope). Wenn eine Antenne eine Verstärkung von mehr als 1 in eine bestimmte Richtung hat, muss sie eine Verstärkung von weniger als 1 in andere Richtungen haben, da die Antenne Energie einspart.
- **Ausrichtung:** Die Form des Übertragungsmusters. Wenn der Antennengewinn erhöht wird, nimmt der Abdeckungsbereich ab. Der Abdeckungsbereich oder das Strahlungsmuster werden in Grad gemessen. Diese Winkel werden in Grad gemessen und als Strahlbreiten bezeichnet. **Hinweis:** Die Strahlbreite ist definiert als ein Maß für die Fähigkeit einer Antenne, die Funkenergie auf eine bestimmte Richtung im Raum zu fokussieren. Die Strahlbreite wird in der Regel in Grad HB oder Horizontal Beamwidth ausgedrückt, meist die wichtigste mit VB als Vertical Beamwidth (nach oben und unten) Strahlungsmuster. Wenn Sie ein Antennenfeld oder -muster anzeigen, wird der Winkel in der Regel an Halbleistungspunkten (3 dB) der Hauptkeule gemessen, wenn er auf die effektive Spitzenleistung der Hauptkeule verweist.
- **Polarisierung:** Die Ausrichtung des elektrischen Feldes der elektromagnetischen Welle durch den Raum. Antennen können horizontal oder vertikal polarisiert werden, obwohl andere Polarisationsarten verfügbar sind. Beide Antennen in einem Link müssen über dieselbe Polarisation verfügen, um einen zusätzlichen unerwünschten Signalverlust zu vermeiden. Um die Leistung zu verbessern, kann eine Antenne manchmal gedreht werden, um die Polarisation zu verändern und so Störungen zu reduzieren. Eine allgemeine Faustregel besagt, dass eine vertikale Polarisierung besser ist, als Funkwellen in Betonschluchten zu senden, und eine horizontale Polarisierung ist in der Regel besser für die Verteilung von Weitverkehrsräumen geeignet. Die Polarisierung kann auch zur Optimierung von HF-Überleitungen eingesetzt werden, wenn die Reduzierung der HF-Energie auf benachbarte Strukturen wichtig ist. Die meisten Rundstrahlantennen werden standardmäßig mit vertikaler Polarisation ausgeliefert. Die von einer Antenne abgestrahlte Funkenergie wird als effektive isotropische Strahlung (EIRP) bezeichnet. Der EIRP-Wert wird in der Regel in Watt oder dBm ausgedrückt. Um eine gerechte und gerechte Aufteilung der nicht lizenzierten Frequenzbänder zu ermöglichen, legen die Zulassungsdomänen maximale EIRP-Stufen fest. Da der EIRP eine Messgröße für die Leistung der Antenne ist, muss der EIRP den Antennengewinn und den Kabelverlust zusammen mit der Sendeleistung enthalten. Antennenkabel können Verluste hinzufügen, was zu einer Dämpfung des übertragenen Signals führt. Je länger das Kabel ist, desto größer ist die Abschwächung und desto größer der Signalverlust im Kabel, der sowohl die Empfangs- als auch die Übertragungsleistung beeinflusst. Die Dämpfung der Kabel hängt von der Qualität und dem Hersteller ab. Verlustarme Kabel liegen in der Regel bei etwa 6,7 dB pro 30 m bei 2,4 GHz (100 Fuß).

Signaldämpfung

Eine Signaldämpfung oder Signalverlust tritt auf, wenn ein Funksignal ein beliebiges Medium durchläuft. Die Signaldämpfung hängt vom Material ab, durch das ein Signal geleitet wird. **Tabelle 2** enthält Werte für Signalverluste für verschiedene Objekte.

Tabelle 2: Signaldämpfungswerte über verschiedene Objekte

Objekt in Signalpfad	Signaldämpfung durch Objekt
Plasterboard-Wand	3 dB
Glaswand mit Metallrahmen	6 dB
Wandhalterung	4 dB
Office-Fenster	3 dB
Metalltür	6 dB
Metalltür in Ziegelwand	12 dB
Körperkörper	3 dB

Hinweis: Dies ist nur eine grobe Anleitung. In verschiedenen Ländern gibt es verschiedene Bauvorschriften. Die unterschiedlichen Vorschriften gelten für den zulässigen Höchstwert für EIRP sowie für andere Parameter.

Eine Übertragungsleistung von 20 mW entspricht 13 dBm. Wenn die an der Einstiegswand einer Gipsplatte übertragene Leistung bei 13 dBm liegt, wird die Signalstärke beim Verlassen dieser Wand auf 10 dBm reduziert.

Standortuntersuchungen an verschiedenen Standorten zeigen unterschiedliche Ebenen von Multipath-Verzerrung, Signalverlust und Signalrauschen an. Krankenhäuser sind aufgrund hoher Multipath-Verzerrung, Signalverlusten und des Rauschens von Signalen in der Regel die anspruchsvollste Umgebung für die Untersuchung. Krankenhäuser benötigen in der Regel mehr Zeit für die Erhebung und benötigen wahrscheinlich eine höhere Bevölkerungsdichte an APs. Auch in der Fertigung und im Ladengeschäft sind Standortuntersuchungen äußerst schwierig. Diese Standorte haben in der Regel einen hohen Metallgehalt in ihrer Gebäudestruktur, was zu reflektierten Signalen führt, die Multipath-Verzerrung wiedergeben. Bürogebäude und Beherbergungsstätten weisen in der Regel eine hohe Signaldämpfung auf, sind aber weniger verzerrt. Die einzige Möglichkeit, die Entfernung zu bestimmen, über die ein Funksignal in einer bestimmten Umgebung gesendet wird, besteht in der Durchführung einer entsprechenden Standortuntersuchung.

Hinweis: Es ist wichtig, die Rx-Signalstufe auf dem AP und den verfolgten Geräten zu berücksichtigen, und nicht so sehr die des Clients, der die Standortbefragungsdaten erfasst. Eine gute Faustregel ist, dass die Access Points bei einer Standortuntersuchung auf eine relativ hohe Leistung eingestellt werden, z. B. auf 50 mW. Da die meisten Antennen symmetrische Tx/Rx-Merkmale aufweisen, spiegeln die sich daraus ergebenden Abdeckungsmuster den ungefähren RSSI der Access Points wider.

Überwachung von Mehrstöckigen Gebäuden, Krankenhäusern und Lagerhäusern

Es gibt eine Vielzahl von Faktoren, die bei der Umfrage von Gebäuden mit mehreren Etagen, Krankenhäusern und Lagerhäusern berücksichtigt werden müssen.

Es ist wichtig, möglichst viele Details in Bezug auf den Bau des Gebäudes zu finden. Einige Beispiele für typische Baumethoden und Materialien, die die Reichweite und den Abdeckungsbereich von APs beeinflussen, sind metallische Folien auf Fensterglas, bleites Glas, Stahlverzierte Wände, Zementböden und -wände mit Stahlverstärkung, foliengestützte Isolierung, Treppenschächte und Elevator-Wellen, Rohrleitungen und Vorrichtungen usw. Außerdem können verschiedene Arten und Stufen von Beständen die Funksignalreichweite beeinflussen, insbesondere solche mit hohem Stahl- oder Wassergehalt. Einige Objekte, auf die Sie achten sollten, sind Druckpapier, Karton-Boxen, Heimtiefutter, Farbe, Mineralölerzeugnisse, Motorteile usw. Stellen Sie sicher, dass die Standortuntersuchung zu Spitzenwerten oder zu Zeiten mit höchster Aktivität durchgeführt wird. Ein Lagerhaus mit einem Lagerbestand von 50 % weist eine deutlich andere HF-Bilanz auf als die Einrichtung, die vollständig belegt ist.

Ebenso weist ein nicht belegter Büroraum eine andere HF-Fläche auf als derselbe Bereich, in dem der Raum belegt ist. Obwohl viele Teile der Standortuntersuchung ohne vollständige Belegung durchgeführt werden können, ist es wichtig, die Standortuntersuchung durchzuführen und die Schlüsselwerte zu einer Zeit zu optimieren, in der Menschen anwesend sind und normale Aktivitäten stattfinden.

Je höher die Auslastungsanforderungen und je höher die Benutzerdichte ist, desto wichtiger ist eine durchdachte Diversitätslösung. Wenn mehr Benutzer vorhanden sind, werden mehr Signale auf dem Gerät jedes Benutzers empfangen. Zusätzliche Signale führen zu mehr Wettbewerb, mehr NULL-Punkte und mehr Multipath-Verzerrung. Die Antennenvielfalt am Access Point trägt dazu bei, diese Bedingungen zu minimieren.

Beachten Sie diese Richtlinien, wenn Sie eine Standortuntersuchung für ein typisches mehrstöckiges Bürogebäude durchführen:

- Elevator-Wellen blockieren und reflektieren RF-Signale.
- Lieferräume mit Inventar absorbieren HF-Signale.
- Innenräume mit harten Wänden absorbieren HF-Signale.
- Unterbrechungsräume (Küchen) können durch Mikrowellenherde verursachte 2,4-GHz-Störungen verursachen.
- Testlabore können Interferenzen im 2,4-GHz- oder 5-GHz-Frequenzbereich verursachen. Das Problem der Interferenz besteht darin, dass dadurch der Geräuschpegel erhöht und die SNR (Signal-Rausch-Verhältnis) des empfangenen Signals verringert wird. Eine höhere Rauschuntergrenze reduziert den effektiven Bereich der Access Points.
- Bürozellen nehmen Signale auf und blockieren sie.
- Klassenfenster und -partitionen reflektieren und blockieren RF-Signale.
- Die Badezimmerfliesen können HF-Signale absorbieren und blockieren.
- Konferenzräume benötigen eine hohe AP-Abdeckung, da sie eine hohe Wi-Fi-Nutzung ermöglichen.

Wenn Sie mehrere Gebäude befragen, können sich APs auf verschiedenen Etagen genauso einfach gegenseitig stören wie APs auf derselben Etage. Dies kann bei der Bereitstellung von Sprach- und/oder Datenanwendungen von Vorteil sein, führt jedoch zu Problemen bei der Bereitstellung von kontextsensitiver Unterstützung. Die Trennung der Böden ist für den ordnungsgemäßen Betrieb dieser Lösung entscheidend. In Gebäuden mit mehreren Tenants kann es zu Sicherheitsbedenken kommen, die die Verwendung von Antennen mit niedrigerer Übertragungsleistung und geringerem Gewinn erfordern, um Signale aus Räumen oder Büros in der Nähe zu verhindern. Der Befragungsprozess für ein Krankenhaus ist in etwa derselbe wie für ein Unternehmen, aber die Anordnung einer Krankenhauseinrichtung unterscheidet sich tendenziell in folgenden Punkten:

- Krankenhausgebäude haben oft wiederkehrende Rekonstruktionen und Ergänzungen. Jede zusätzliche Konstruktion kann unterschiedliche Baumaterialien mit unterschiedlichen Signaldämpfungsstufen erfordern.
- Die Signaldurchdringung durch Wände und Böden in den Patientenbereichen ist in der Regel minimal, was zur Bildung von Mikrozellen beiträgt. Daher muss die AP-Dichte deutlich höher sein, um eine ausreichende Funkabdeckung zu gewährleisten.
- Der Bedarf an Bandbreite steigt mit der verstärkten Nutzung von WLAN-Ultraschallgeräten und anderen tragbaren Bildverarbeitungsanwendungen.
- Da eine höhere AP-Dichte erforderlich ist, können sich Zellen-Überschneidungen stark auswirken, was zu einer Wiederverwendung der Kanäle führt.
- In Krankenhäusern können verschiedene Arten von Wireless-Netzwerken installiert sein, darunter Geräte mit 2,4 GHz (nicht 802.11-konformer Qualität). Dieses Gerät kann Konflikte mit anderen 2,4-GHz- oder 5-GHz-Netzwerken verursachen.
- Patchantennen für die Wandmontage und Rundstrahlantennen für die Diversität an der Decke sind beliebt, aber beachten Sie, dass eine Vielfalt an Antennen erforderlich ist.

Die Lagerhäuser verfügen über große offene Bereiche, in denen häufig hohe Lagerbestände vorhanden sind. In vielen Fällen reichen diese Racks fast bis an die Decke, wo in der Regel APs platziert werden. Solche Storage-Racks können den Bereich begrenzen, den der Access Point abdecken kann. In diesen Fällen sollten Sie APs an anderen Stellen außerhalb der Decke platzieren, z. B. an Seitenwänden und Zementsäulen. Berücksichtigen Sie auch bei der Umfrage eines Lagers folgende Faktoren:

- Die Bestandsebenen beeinflussen die Anzahl der benötigten Access Points. Testabdeckung mit zwei oder drei APs an geschätzten Platzierungsorten.
- Unerwartete Zellüberschneidungen sind wahrscheinlich durch Abdeckungsschwankungen bedingt. Die Qualität des Signals variiert mehr als die Stärke des Signals. Die Clients können APs, die weiter entfernt liegen, mit APs verbinden und besser arbeiten als APs in der Nähe.
- Während einer Umfrage verfügen APs und Antennen in der Regel nicht über ein Antennenkabel, das sie miteinander verbindet. In einer Produktionsumgebung können APs und Antennen jedoch Antennenkabel erfordern. Alle Antennenkabel haben einen Signalverlust. Die genaueste Umfrage bezieht sich auf die Art der zu installierenden Antenne und die Länge des zu installierenden Kabels. Ein gutes Tool zur Simulation des Kabels und sein Verlust ist ein Dämpfer in einem Umfragekit.

Wenn Sie eine Fertigungsstätte befragen, ähnelt dies der Überwachung eines Lagers. Ein Hauptunterschied besteht darin, dass die umgebende Funkumgebung in einer Fertigungsstätte aufgrund einer Vielzahl weiterer Störungsquellen viel lauter ist. Darüber hinaus benötigen Anwendungen in einer Fertigungsanlage in der Regel mehr Bandbreite als Anwendungen in einer Lagerumgebung. Diese Anwendungen können Videoaufnahmen und drahtlose Sprachübertragungen umfassen. Multipath-Verzerrung ist wahrscheinlich das größte Leistungsproblem in einer Fertigungsanlage.

Es ist wichtig, dass die Standortuntersuchung nicht nur die Signalpegel misst, sondern auch Pakete generiert und anschließend Paketfehler meldet, um die Funkumgebung korrekt zu charakterisieren.

Für Bereiche mit hohem Benutzerdatenverkehr, z. B. Büroflächen, Schulen, Einzelhandelsgeschäfte und Krankenhäuser, empfiehlt Cisco, den Access Point außerhalb des Sichtbereichs zu platzieren und unauffällige Antennen unter die Decke zu stellen.

Standortrollen und Regionen

Die Bereitstellungsrichtlinien bieten eine gute Genauigkeit: 10 m/90 %, 5 m/50 %. Der Wert von 10 m/90 % entspricht einem Radius von 10 m vom tatsächlichen physischen Standort eines Geräts. Es gibt also Fälle, in denen diese Genauigkeitsziele erreicht werden. Das nachverfolgte Gerät kann jedoch in Bereichen auf Boden- und/oder Gebäudeebene angezeigt werden, in denen keine Geräte vorhanden sind.

Die Funktion "Rails and Regions" bietet Netzwerkadministratoren die Möglichkeit, Bereiche für die Einbindung/Ausschluss von Standortdiensten zu definieren. Mit dieser Funktion können bestimmte Regionen auf einer Karte innerhalb oder außerhalb des Gültigkeitsbereichs eines gültigen Standortbereichs definiert werden.

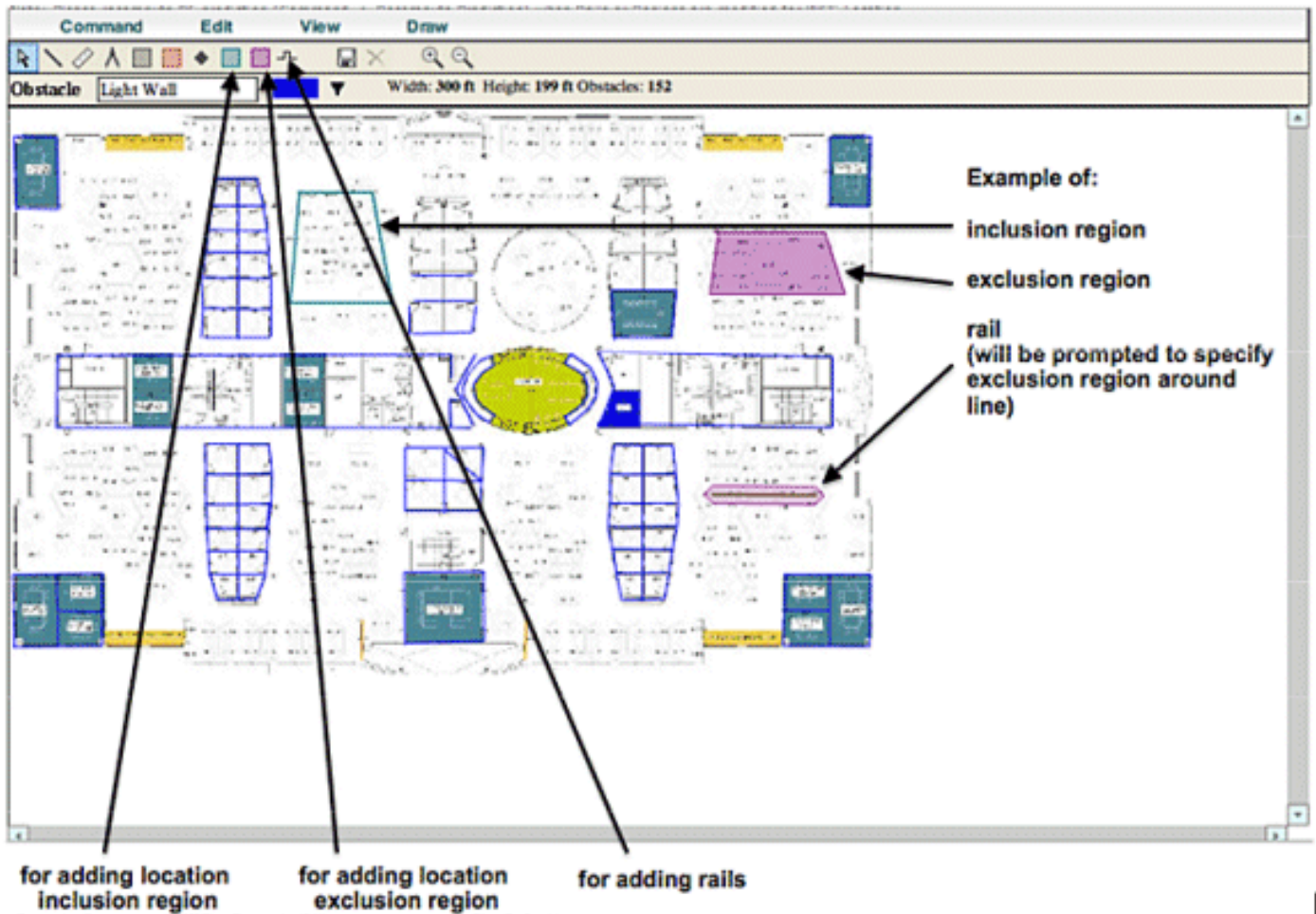
Es können drei Arten von Bereichen angegeben werden, wie in **Abbildung 14** gezeigt:

- **Region für Standortinklusion:** Das verfolgte Gerät darf sich nicht außerhalb dieses Polygons befinden (Beispiel: außerhalb der Außenwände)
- **Standort-Ausschlussregion:** Das verfolgte Gerät darf nicht in diesem Polygon enthalten sein (Beispiele: offenes Atrium oder Gebäudesperren). Die Ausgrenzung wird gegenüber der Einbeziehung in den Fall bevorzugt, dass gegensätzliche Regionen gezogen werden.
- **Schienen:** Das verfolgte Gerät muss innerhalb eines definierten Bereichs mit schmalen Band liegen, der in der Regel innerhalb der Sperrzone verwendet wird (Beispiel: Förderband).

Nachdem die Bereiche Rails und Region im WCS definiert wurden, muss die Bodenaktualisierung vom WCS über den Synchronisierungsprozess an die MSE übertragen werden.

Hinweis: Auf der MSE arbeiten Standortläufe und Regionen nur mit kontextsensitiver Engine für Clients. AeroScout hat eine Funktion namens Zellen und Masken implementiert, die ähnliche Funktionen für die Nachverfolgung von Tags bietet. Bei der Cisco 2710 Location Appliance kann die Funktion "Rails and Regions" sowohl mit Client- als auch mit Tag-Verfolgung verwendet werden.

Abbildung 14: Schienen und Regionen

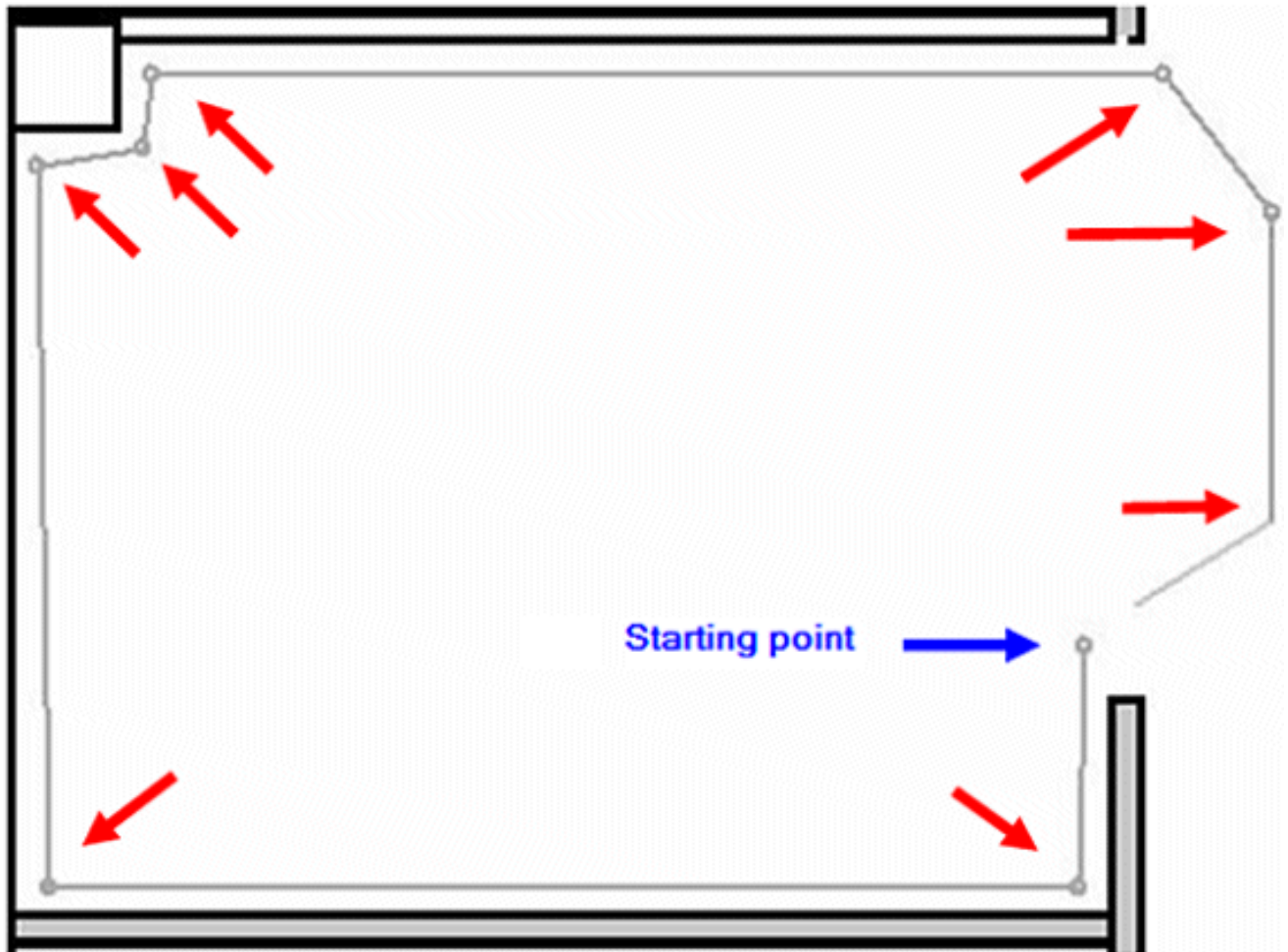


Erstellen einer Maske im System Manager

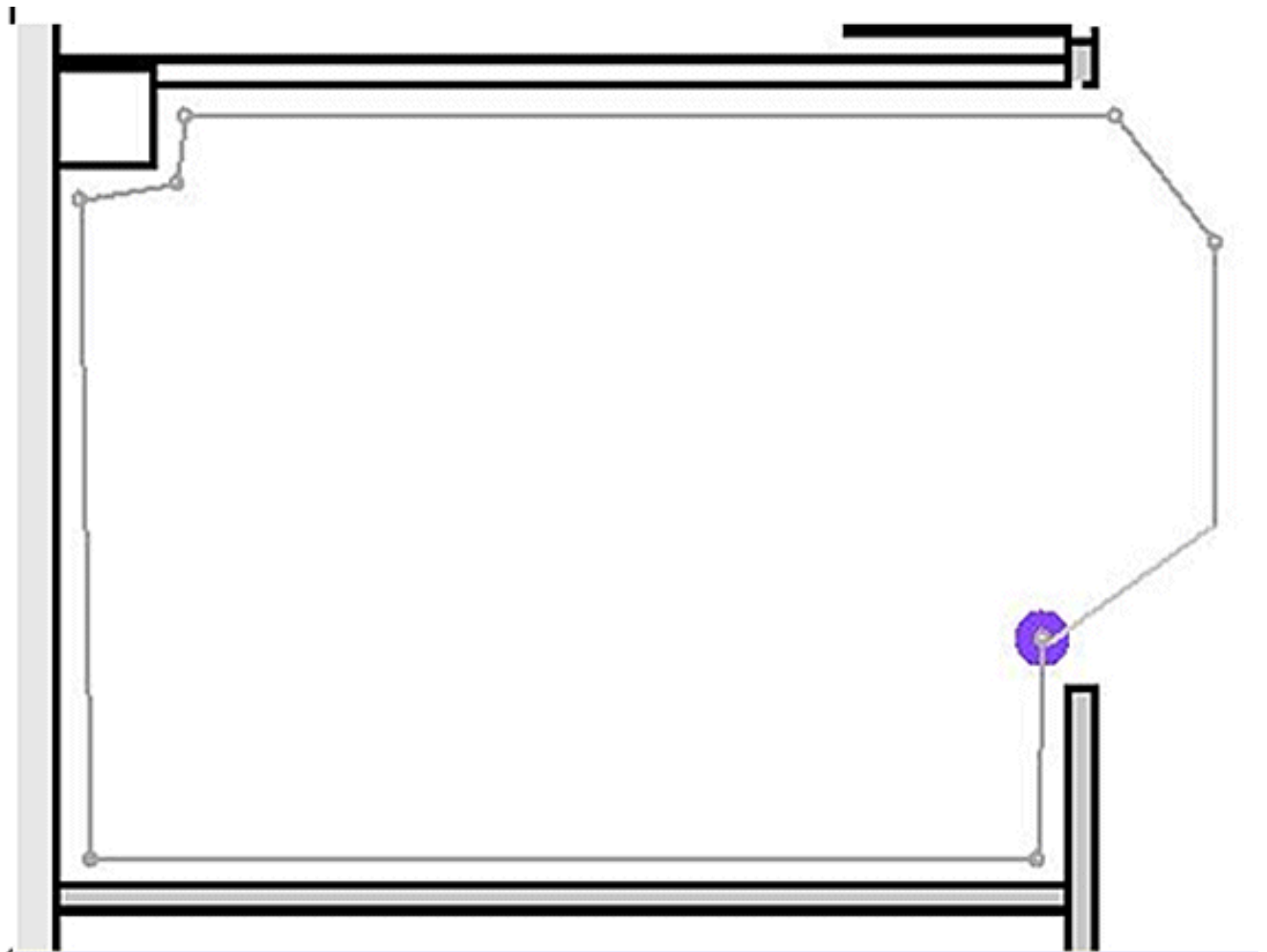
Eine Maske wird durch Zeichnen eines Polygons auf einer Karte definiert, die den auszuschließenden Bereich abgrenzt.

Gehen Sie wie folgt vor, um eine Maske zu erstellen:

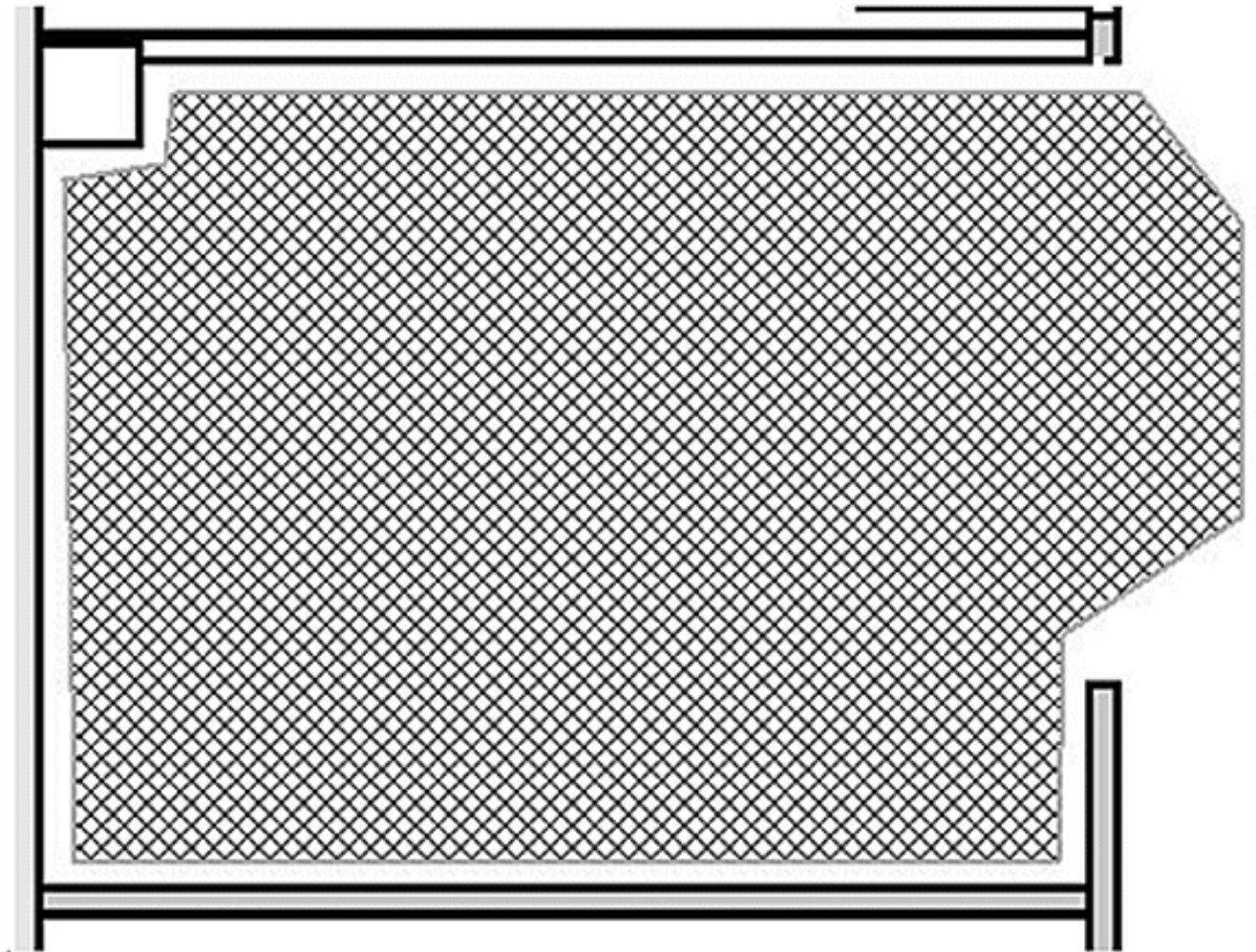
1. Wählen Sie **Konfiguration, Karten, Maske und Maske bearbeiten aus**. Dadurch wird das System in den Maskenbearbeitungsmodus umgeschaltet. Der Mauszeiger wird zu einem Kreuz.
2. Klicken Sie auf einen Punkt auf der Karte. Schieben Sie die Maus an den nächsten Punkt, klicken Sie erneut, und wiederholen Sie diesen Vorgang, um die Verzerrungen des Polygons zu kennzeichnen (siehe **Abbildung 15**). **Abbildung 15: Erstellen einer Maske - Markieren der Stellen im Polygon**



Wenn Sie die Maus an den Startpunkt schieben, wird zum Schließen des Polygons ein violetter Kreis angezeigt, der den Endpunkt anzeigt (siehe **Abbildung 16**).**Abbildung 16: Erstellen einer Maske: Der violette Kreis gibt den Endpunkt an.**



Klicken Sie, um die Maskendefinition abzuschließen. Die Maske wird auf der Karte angezeigt (siehe Abbildung 17).**Abbildung 17: Erstellen einer Maske - Die Maske wird auf der Karte angezeigt.**



3. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle der Karte, und wählen Sie **Maskenziehungsmodus verlassen** (oder drücken Sie **Esc**), um den Maskenbearbeitungsmodus zu beenden. Standardmäßig wird die Maske aus dem Display entfernt, nachdem sie den Maskenziehungsmodus verlassen hat. Weitere Informationen zum Aktivieren/Deaktivieren oder Bearbeiten von Masken finden Sie in der [Aeroscout-Dokumentation](#).

Zellen in kontextsensitiver Engine für Tags

Zellen sind so konzipiert, dass sie eine Karte in kleinere Teile aufteilen, um den Prozess der Standortberechnung zu optimieren und die Positionierungsgenauigkeit zu verbessern. Die Zelle definiert die geografischen Grenzen für die Positionierung eines Tags. Außerdem wird definiert, welche bestimmten Geräte (TDOA-Empfänger und Access Points) am Standortberechnungsprozess innerhalb dieser Grenzen beteiligt sind.

Der Zellmechanismus wird sowohl für RSSI- als auch für TDOA-Standortberechnungen verwendet.

Die Engine verarbeitet eingehende Standortdaten:

- Ein Bericht, der die Position eines Tags angibt, kann gleichzeitig von mehreren Access Points oder Wi-Fi-TDOA-Empfängern stammen. Die Karten-Differenzierungsalgorithmen des Motors wählen die Karte aus, auf der sich das Gerät am ehesten befindet, und verwerfen Standortberichte, die auf andere Karten zeigen.
- Sobald die Karte bestimmt ist, sucht die Engine nach Zellen. Wenn die Karte in Zellen

unterteilt ist, wählt derselbe Optimierungsmechanismus die Zelle aus, die die TDOA-Empfänger/Access Points der Zellen empfängt, die am ehesten den genauen Standortbericht geliefert haben. Der Standort des Geräts wird dann anhand der Daten berechnet, die von den TDOA-Empfängern/Access Points, die dieser Zelle zugeordnet sind, innerhalb der Grenzen dieser Zelle empfangen wurden.

Beachten Sie, dass die TDOA-Empfänger/Access Points, die einer Zelle zugeordnet sind, sich nicht notwendigerweise innerhalb des durch die Zellgrenzen begrenzten Bereichs befinden müssen.

Erstbetrieb bei Zellenkonfiguration

Zunächst wird automatisch eine Standardzelle für jede Karte erstellt, um den gesamten Kartenbereich abzudecken. Führen Sie folgende Schritte aus, um die Zuordnung in separate Zellen aufzuteilen:

1. Bearbeiten Sie die Standardzelle, um nur eine Teilmenge des Kartenbereichs abzudecken (siehe Anleitungen zum Ändern einer Zelle).
2. Fügen Sie der Karte nach Bedarf weitere Zellen hinzu. Beachten Sie, dass eine Zelle nicht vollständig in eine andere Zelle eingeschlossen werden kann.
3. Gehen Sie die Eigenschaften der einzelnen Standortgeräte (Access Points und TDOA-Empfänger) durch, und ordnen Sie das Gerät den richtigen Zellen zu.
4. Die zugeordneten Geräte einer Zelle dürfen keine Teilmenge der zugeordneten Geräte einer anderen Zelle sein. Stellen Sie sicher, dass jeder Zelle Geräte zugeordnet sind, die keiner anderen Zelle zugeordnet sind.

Kalibrierung - kontextsensitive Engine für Clients

Die Standortgenauigkeit hängt von zwei Hauptfaktoren ab:

- AP-Platzierung und Anzahl der APs, die zum Standort beitragen
- Korrekte Funksignalmerkmale eines AP für eine bestimmte Umgebung (genaue AP-Wärmezuordnung)

Während der Kalibrierungsphase werden Daten auf dem WCS-Server erfasst, wenn ein Rundgang durch die Zielumgebung mit einem Mobilgerät durchgeführt wird, mit dem mehrere APs die Signalstärke dieses Geräts ermitteln können. Die empfohlene Methode besteht darin, einzelne oder mehrere Laptops zu verwenden, die bei WCS angemeldet sind (maximal fünf Geräte pro Funkband), und eine Karte des zu kalibrierenden Bereichs auszuwählen, die in der Regel mit einer Reihe von Rasterpunkten oder Notationen überlagert wird, um den Bediener zu befähigen, genau zu bestimmen, wo Stichprobendaten erfasst werden müssen. An jedem Stichprobenpunkt auf der Karte wird der RSSI-Satz, der dem Kalibriergerät zugeordnet ist, vom WLC an die MSE weitergeleitet. Die Größe eines bestimmten Datensatzes basiert auf der Anzahl der empfangenden Access Points, die das mobile Gerät erkennen. Aufgrund von verblassten und anderen HF-Umgebungsmerkmalen ist die beobachtete Signalstärke eines Mobilgeräts an einem bestimmten Standort eine Zeitvariante, d. h., sie kann sich mit der Zeit ändern. Daher werden viele Datenproben für ein Kalibriergerät im Kalibrierprozess aufgezeichnet.

Jede Umgebung ist einzigartig, und die Signalmerkmale eines Access Points in einer bestimmten Umgebung variieren erheblich. WCS stellt einen Mechanismus bereit, mit dem Benutzer Signalmerkmale für ihre Umgebung kalibrieren können. Der erste Schritt zur Optimierung der Genauigkeit besteht darin, sicherzustellen, dass die AP-Bereitstellung den zusammengefassten

Standortbereitstellungsrichtlinien entspricht. Der Versuch, die Standortgenauigkeit durch eine Kalibrierung mit unzureichender AP-Abdeckung und -Platzierung zu verbessern, führt möglicherweise nicht zu adäquaten Ergebnissen und kann sogar der Genauigkeit abträglich sein.

Mit WCS werden drei Standard-Kalibriermodelle bereitgestellt:

- Kuben und geschlossene Büros
- Nur für Trockenbüros
- Freier Raum

Jedes Modell basiert auf den gängigsten Faktoren in einer typischen Kundenumgebung. Das erste dieser beiden RF-Modelle ist in einer normalen Büroumgebung nützlich.

Wenn die bereitgestellten RF-Modelle die Bodengestaltung nicht ausreichend charakterisieren, können Kalibriermodelle mit WCS erstellt und auf den Boden angewendet werden, um die Dämpfungsmerkmale einer bestimmten Umgebung besser darzustellen. In Umgebungen, in denen viele Etagen gemeinsame Dämpfungsmerkmale aufweisen, kann ein Kalibriermodell erstellt und dann auf alle ähnlichen Stockwerke angewendet werden.

In einigen Innenbereichen kann die Dämpfung höher sein als in einer typischen Büroumgebung. In entsprechend konzipierten Innenanlagen, in denen eine höhere Dämpfung zu einer weniger optimalen Standortgenauigkeit beitragen kann, kann eine Standortkalibrierung dazu beitragen, weniger als optimale Leistung wiederherzustellen. Wenn eine Vor-Ort-Kalibrierung durchgeführt wird, kann das System Pfadverluste von bekannten Punkten in der gesamten Umgebung untersuchen, wodurch es in der Lage ist, ein benutzerdefiniertes RF-Modell zu erstellen, das ein besseres Verständnis der für die Umgebung spezifischen Verbreitungsmerkmale ermöglicht.

In vielen Fällen kann die Verwendung der bei der Kalibrierung gesammelten Informationen anstelle eines Standardmodells den Fehler zwischen berechneter Clientposition und empirischen Daten drastisch reduzieren. In Umgebungen, in denen viele Etagen fast identische Dämpfungsmerkmale aufweisen, ermöglichen starke Ähnlichkeiten zwischen diesen Standorten die Anwendung des RF-Modells, das durch Kalibrierung an einem der Standorte erstellt wurde, auf andere ähnliche Bereiche mit guten Ergebnissen.

Ebenfalls zu berücksichtigen sind Bereiche mit gemischter HF-Dämpfung, d. h. Fertigungs- oder Lagerhäuser, in denen stapelbare Güter oder eine dichte Behinderung in einem Bereich des Gebäudes und/oder der für Montage oder Versand genutzten freien Räume vorhanden sein können. Diese Bereiche sind als unabhängige Zonen zu behandeln, die die Kalibrierung auf die Bereiche beschränken, in denen höchste Genauigkeit erforderlich ist. Wenn für alle diese Bereiche in einem gemischten Bereich höchste Genauigkeit erforderlich ist, ist es ratsam, die Bodenfläche in einzelne Zellen oder Karten zu unterteilen und separate RF-Modelle anzuwenden.

Hinweis: Die Leistung dieser Art von RF-Modellen ist komplex und erfordert weitere Überlegungen zur Bereitstellung, die nicht in diesem Dokument behandelt werden.

Die Kalibrierung ist in der Tat ein mehrstufiger Prozess, der mit der Definition eines neuen Kalibriermodells durch **Monitor > Maps > RF Kalibriermodelle > Create New Model** beginnt. Eine schrittweise Beschreibung des Kalibrierungsprozesses finden Sie unter *Erstellen und Anwenden von Kalibrierungsmodellen* im [Cisco Context-Aware Software Configuration Guide](#).

Im Kalibrierprozess überträgt der Kalibrierclient wiederholt Anfragen auf allen Kanälen. Je nach verwendetem Kalibrierclient kann der Client angestoßen werden, um über eine Netzwerkanfrage auf Anfrage Anfragen zu senden. Clients, die diese Anforderungen nicht erkennen können,

können deauthentifiziert und getrennt werden, um Anfragen an das Wireless-Netzwerk zu senden und anschließend erneut zuzuordnen/zu authentifizieren. Access Points in der Nähe des Clients erkennen den RSSI dieser Anfragen und geben diese Informationen an ihre registrierten Controller weiter. Controller stellen dem WCS die im Kalibrierprozess erfassten RSSI-Informationen zur Verfügung, um die Pfadverluste zu berechnen, die zur Definition des neuen Kalibriermodells verwendet werden.

Beim Erstellen eines Kalibriermodells besteht der entscheidende Schritt darin, die Datenpunkte zu sammeln. Die Datenpunkterfassungsphase des Kalibrierprozesses im WCS kann mit einer von zwei Methoden durchgeführt werden. Sie kann über ein einzelnes internetfähiges Mobilgerät ausgeführt werden, das dem WLAN zugeordnet ist und sowohl die Überprüfung des Netzwerks als auch die eigentliche Datensammlung steuert. Alternativ kann die Datenerhebungsphase von zwei separaten Geräten aus durchgeführt werden, die der WLAN-Infrastruktur zugeordnet sind. In diesem Fall wird die Interaktion mit der WCS-GUI von einem primären Gerät gesteuert, das mit Tastatur- und Mausfunktionen ausgestattet ist. Die eigentliche Generierung von Anfragen erfolgt auf einem zweiten zugeordneten Gerät, wenn Sie die bekannte MAC-Adresse auswählen.

Es wird empfohlen, die Kalibrierdaten für jedes Band einzeln zu erfassen. Wenn Sie einen Dual-Band-Client verwenden, verwenden Sie eine der folgenden Alternativen:

1. Führen Sie die Kalibrierdatensammlung mit einem einzelnen Laptop mit einem Cisco Aironet 802.11a/b/g Wireless CardBus Adapter (AIR-CB21AG) auf jedem Band einzeln durch. Wenn Sie eine Kalibrierung für das 2,4-GHz-Band durchführen, deaktivieren Sie das 5-GHz-Band, und schließen Sie die Datensammlung nur mit dem 2,4-GHz-Band ab. Nach Abschluss dieses Kalibrierprozesses sollte das 2,4-GHz-Band deaktiviert, das 5-GHz-Band aktiviert und der Prozess zur Kalibrierdatensammlung mit dem 5-GHz-Band wiederholt werden. **Hinweis:** In einer Produktionsumgebung, in der sich die Auswahl des PC-Funkbands als schwierig erweist, empfiehlt es sich, eine spezifische Kalibrier-SSID mit nur 11b/g oder 11a aktiv zu definieren.
2. Kalibrierung mit bis zu fünf Clients pro Funkband - jedes mit einem Laptop ausgestattet. Jeder Laptop muss über einen Cisco AIR-CB21AG verfügen und der Infrastruktur mit einem dedizierten Band zugeordnet sein. Jeder Kalibrierclient kann unabhängig arbeiten.

Bevor Sie eine Kalibrierung durchführen, sind mehrere Vorkonfigurationsschritte erforderlich:

1. Informieren Sie in einer Produktionsumgebung das Personal bzw. die Mitarbeiter über den Prozess. Dadurch werden Unterbrechungen reduziert und eine höhere Genauigkeit gewährleistet. Reduzierung des Unfallrisikos insbesondere in Fertigungsbetrieben, in denen Gabelstapler eingesetzt werden.
2. Deaktivieren Sie den dynamischen RRM AP-Stromversorgungsmodus auf den Controllern oder APs, auf denen die Kalibrierung durchgeführt wird.
3. Stellen Sie sicher, dass die Karten im WCS skaliert und die APs korrekt mit der richtigen Antennentypausrichtung und -höhe positioniert werden.
4. Der PC oder das Gerät, der bzw. das für die Kalibrierung verwendet wird, ist mit einem Access Point auf der betreffenden MAP verknüpft.
5. Der für die Kalibrierung verwendete Wireless-Client muss mindestens CCXv2 sein. Cisco empfiehlt CCXv4 für optimale Ergebnisse. Die CCX-Versionsinformationen für Clients können in WCS angezeigt werden (siehe **Abbildung 18**). **Abbildung 18: Überprüfen der CCX-Version von Clients**

Client Details : Client 'Unknown' - Intel:73:22:e3

Monitor > [Clients](#) > Client Details

Properties			
Client User Name	<Unknown>	Controller	171.71.128.78
Client IP Address	128.107.21.101	Port	2
Client MAC Address	00:1d:e0:73:22:e3	Protocol	802.11g
Client Vendor	Intel	SSID	guestnet
CCX	V4	Profile Name	guestnet
Power Save	OFF	AP Name	sjc14-41b-ap4
		AP IP Address	171.71.133.127
		AP Type	Cisco AP
		AP Base Radio MAC	00:17:df:a8:59:40
		Interface	guest
		VLAN ID	240

6. Der Cisco Secure Services Client (CSSC) darf nicht zum Ausführen der Kalibrierung verwendet werden.
7. Auf einer Bodenkarte müssen mindestens 50 Datenpunkte erfasst werden.
8. Nachdem Sie das Kalibriermodell erstellt und dieses Modell auf die Bodenkarten angewendet haben, muss WCS mit MSE synchronisiert werden.

Bei mehrstöckigen Gebäuden muss die Eichdatensammlung jeweils auf einer Etage abgeschlossen sein. Da es die Möglichkeit gibt, dass ein Kalibrierclient von APs auf angrenzenden Stockwerken durch HF-Blutungen zwischen den Etagen gesehen und gesehen werden kann, minimiert die Erfassung von Kalibrierdaten auf einer Etage das Risiko, dass die MSE Kalibrierdaten zwischen den Etagen mischt.

Wenn ein mit CCXv2 oder höher kompatibler Client der WLAN-Infrastruktur zugeordnet und im WCS als Kalibrierclient angegeben ist, wird die MAC-Adresse des Clients in die Einstelltable aller Controller eingefügt, die die im kalibrierten Boden enthaltenen Access Points bedienen. Diese Einfügung erfolgt anfänglich unmittelbar nach Angabe der MAC-Adresse des Kalibrierclients, des Kalibriercampus, des Gebäudes und des Bodens. Nach jeder Speicherung eines erfassten Datenpunkts wird die Client-MAC-Adresse aus der Ortungskalibrierungstabelle des Controllers entfernt. Die Client-MAC-Adresse wird dann bei jeder nachfolgenden Speicherung des Datenpunkts kurz in die Kalibriertabellen am Controller-Standort zurückgesetzt und anschließend sofort entfernt. Dieser Prozess wiederholt sich für jeden gesammelten Datenpunkt.

Wenn die MAC-Adressen von CCXv2-Clients (oder höher) in der Ortungskalibrierungstabelle eines WLC angezeigt werden, werden Unicast Radio Measurement Requests an diese Clients gesendet. Ähnlich wie Rundfunkmessenanfragen dazu beitragen, die Standortgenauigkeit kompatibler Clients im normalen Betrieb zu verbessern, führen Unicast Radio Measurement Requests, die in kurzen regelmäßigen Abständen (4 Sekunden) gesendet werden, dazu, dass kompatible Kalibrierclients Anfragen häufig senden. Durch die Verwendung von CCX Radio Measurement Requests und CCXv2- oder höheren Clients ist dies möglich, ohne dass der Client gezwungen werden muss, die Verbindung zu trennen und erneut zuzuordnen. Dies ermöglicht eine konsistentere und zuverlässigere Überprüfung des Netzwerks und einen reibungsloseren Betrieb des Kalibrierclients, insbesondere wenn er als Workstation verwendet wird, die über die grafische Benutzeroberfläche für die Kalibrierdatenerfassung mit WCS interagiert.

Ein Kalibriermodell wird auf den Boden angewendet und stellt die Dämpfungsmerkmale dieses Bodens besser dar. In Umgebungen, in denen viele Etagen gemeinsame Dämpfungsmerkmale aufweisen, kann ein Kalibriermodell erstellt und dann auf Böden mit demselben physischen Layout und derselben Bereitstellung angewendet werden.

Kalibrierdaten können mit einer von zwei Methoden gesammelt werden:

- **Punktmodus-Sammlung** - Kalibrierpunkte werden ausgewählt, und ihr Abdeckungsbereich wird berechnet, und zwar jeweils an einem Ort (siehe **Abbildung 19** und **20**).
- **Lineare Modusauflistung** - Eine Reihe von linearen Pfaden wird ausgewählt und dann berechnet, wenn Sie den Pfad durchlaufen. Dieser Ansatz ist in der Regel schneller als die Datensammlung. Sie können auch die Datensammlung verwenden, um die Datenerfassung für Orte zu erweitern, an denen die linearen Pfade verpasst haben (siehe **Abbildung 21**).

Obwohl beide Methoden offiziell unterstützt werden, empfiehlt Cisco, den Punktmodus für die Kalibrierung zu verwenden, da dies die besten Ergebnisse liefert.

Abbildung 19: Kalibrierung - Punktmodus

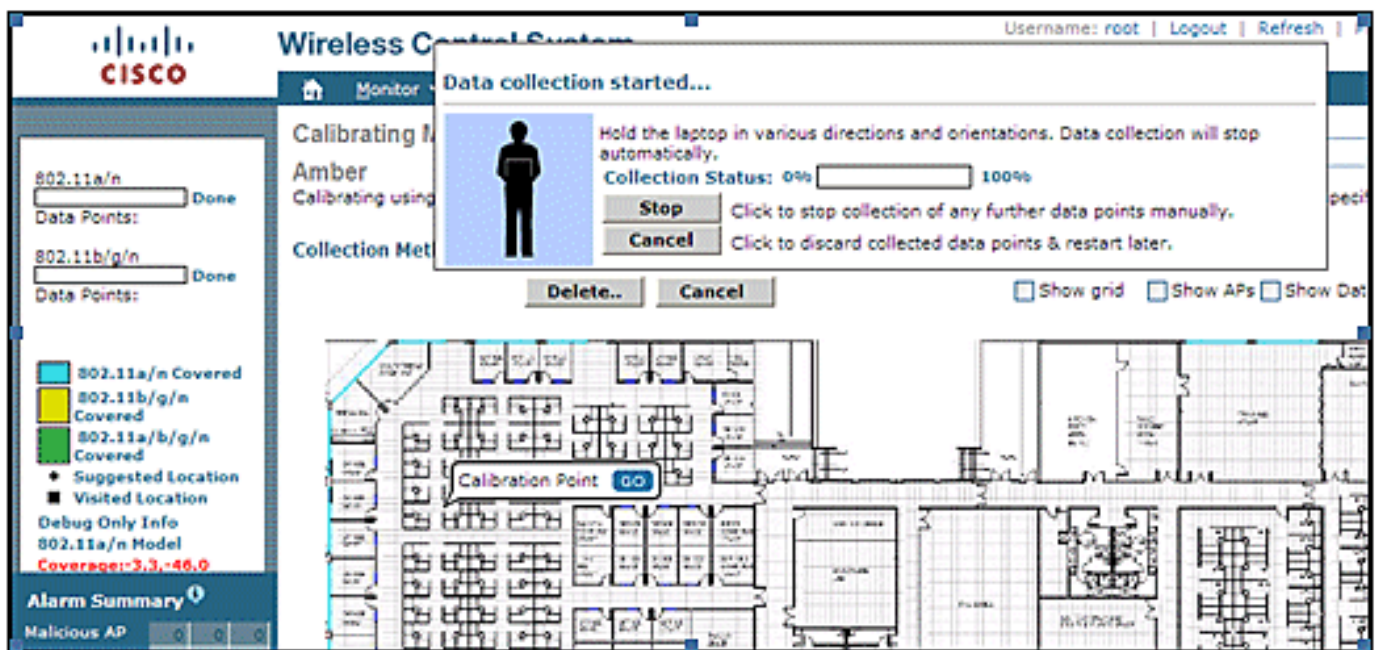


Abbildung 20: Punktmodus - Kalibrierergebnisse

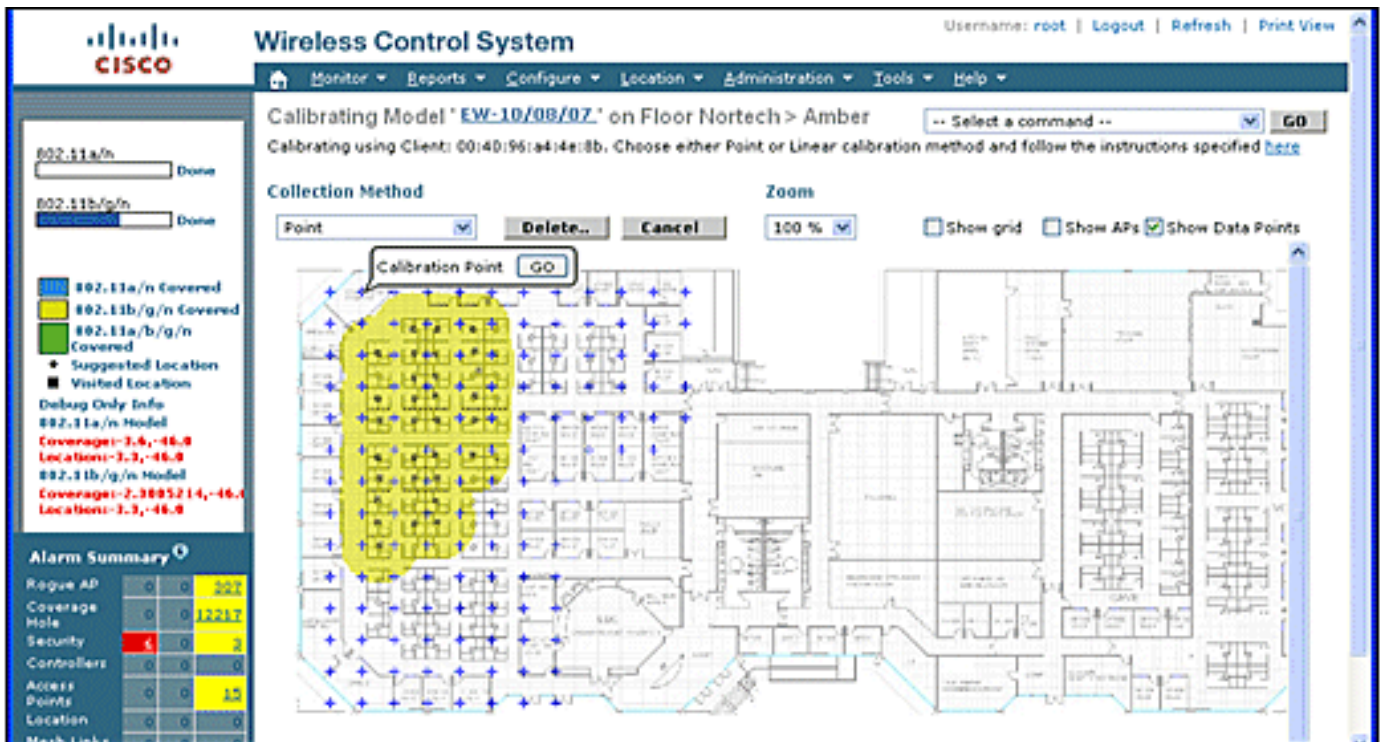
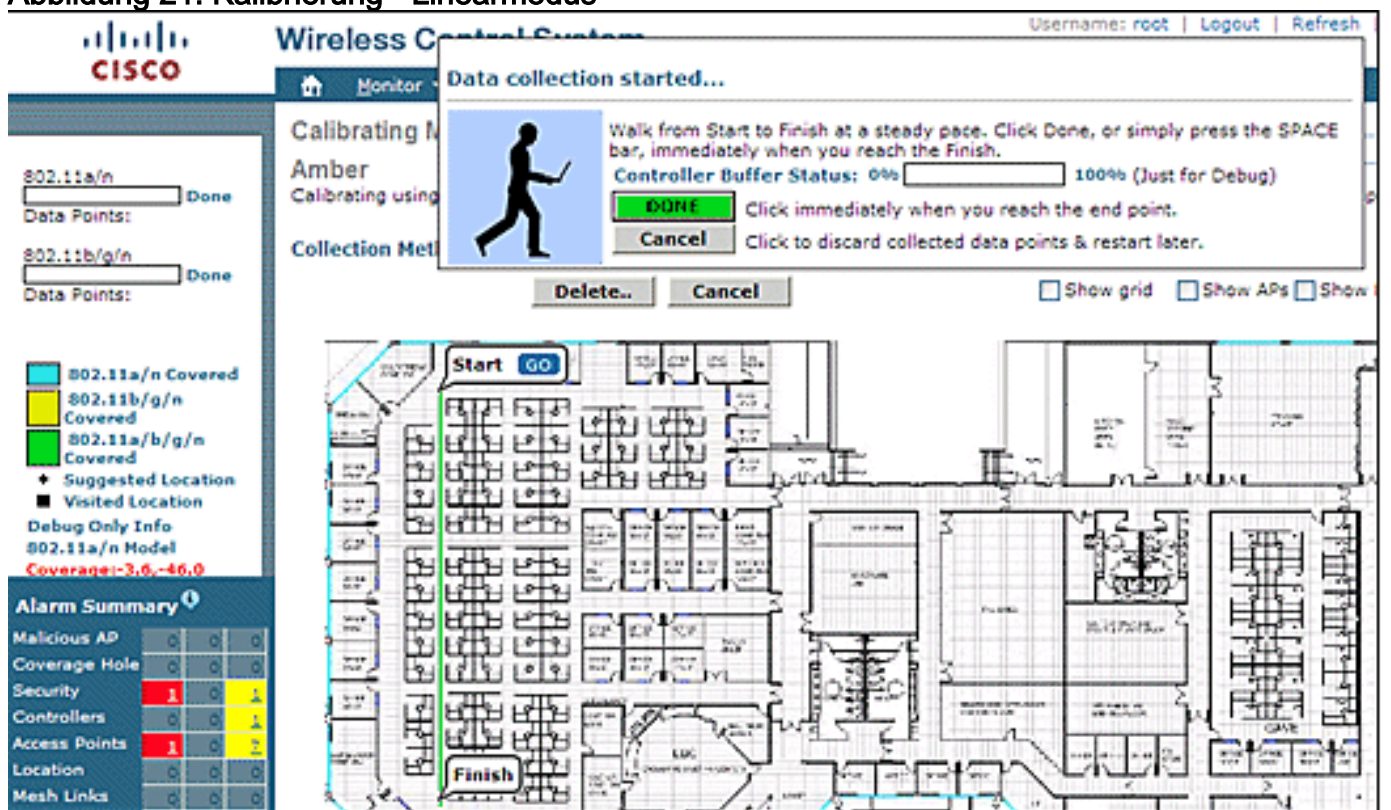


Abbildung 21: Kalibrierung - Linearmodus



Kalibrierungsmodelle können nur auf Clients, nicht autorisierte Clients und nicht autorisierte Access Points angewendet werden. Die Kalibrierung für Tags erfolgt mit dem AeroScout System Manager.

Kalibrierung - kontextsensitive Engine für Tags

Die MSE verfügt über zwei Location Engines: eine zum Nachverfolgen von Clients (im vorherigen Abschnitt beschriebene Cisco Engine) und eine zum Nachverfolgen von Tags (AeroScout). Jeder Motor hat ein separates Kalibriermodell, sodass die Kalibrierung für Tags ein separater Prozess ist.

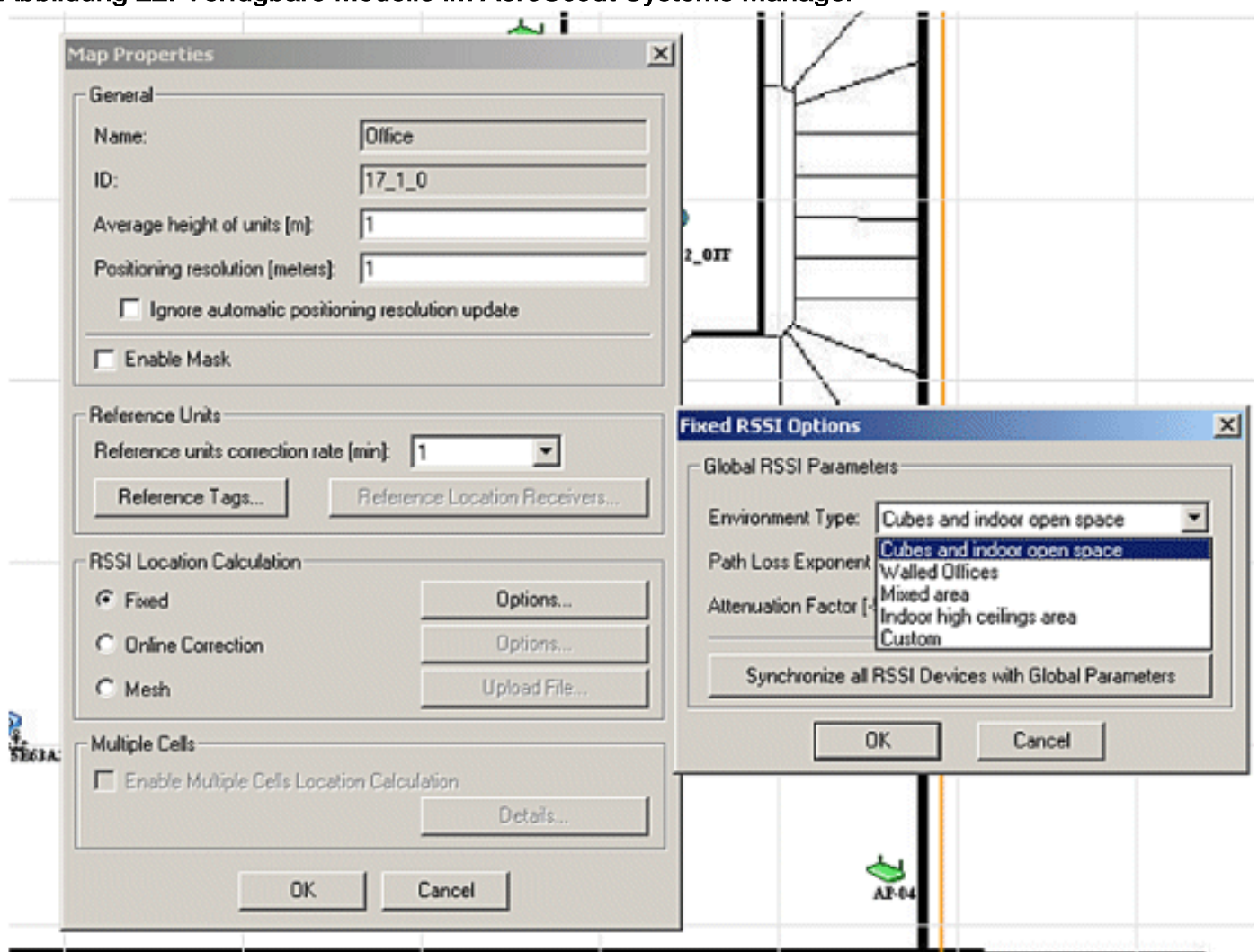
Die AeroScout-Engine setzt für alle importierten WCS-Maps das typische Standard-RF-Path-Verlustmodell für das Büro voraus. Wenn dies nicht Ihre Umgebung darstellt, müssen die Standardmodelle pro Karte und Zelle geändert werden, um die Standortgenauigkeit zu verbessern.

AeroScout System Manager: Um die standardmäßigen PLM-Einstellungen (Path Loss Model) zu ändern, muss die Anwendung AeroScout System Manager installiert und ausgeführt werden. Informationen zum Herunterladen und Installieren finden Sie in der [AeroScout-Dokumentation](#).

Melden Sie sich nach dem Start der Anwendung bei der MSE-Engine an, wechseln Sie zum eigentlichen Kartenboden, der modifiziert werden muss. Wechseln Sie mit der Pulldown-Registerkarte zu **Konfiguration > Zuordnung > Eigenschaften**. Mithilfe der RSSI-Standortberechnungsoptionen kann der feste Umgebungstyp ausgewählt werden, der den physischen Spezifikationen entspricht, die durch die vier in **Abbildung 22** dargestellten definierten Modelle dargestellt werden. Nachdem Sie das Modell gewählt haben, wenden Sie es auf die gewählte Etage an. Verwenden Sie die Registerkarte **OK** oder die Option zur **Synchronisierung aller RSSI-Geräte mit globalen Parametern**, die dasselbe Modell auf alle vorhandenen Karten wie das neue Standardmodell überträgt.

Hinweis: Die fünfte Option, "Custom" (Benutzerdefiniert), darf nur verwendet werden, wenn sie von AeroScout oder dem technischen Support von Cisco angefordert wird.

Abbildung 22: Verfügbare Modelle im AeroScout Systems Manager



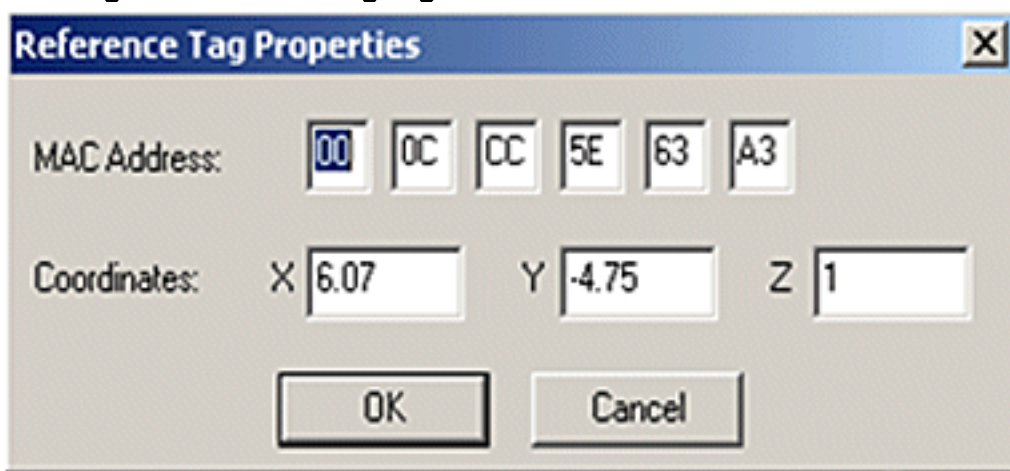
Kalibriermethoden - Es stehen mehrere Optionen für einzelne Tags als statische Referenzgeräte

zur Verfügung, oder wenn regelmäßige oder einmalige Aufzeichnungen durchgeführt werden, die zur Analyse und Berechnung präziser Modelle pro Karte/Zelle verwendet werden können.

Referenztags - Dies sind Standardtags für die Ressourcenverfolgung. Der einzige Unterschied, wenn überhaupt, ist die Konfiguration. Normalerweise verwendet ein Referenztag für ein definiertes Messintervall einen schnelleren Beacon-Zeitraum.

Referenztags können mit der MAC-Adresse definiert werden (siehe **Abbildung 23**) und direkt auf eine Zelle oder Karte platziert werden, die durch ein blauer verankerter Tag angezeigt wird. Die Koordinaten können manuell durch einen Rechtsklick auf die Karte eingegeben werden. Referenztags, die für die dynamische Anpassung des Standorts verwendet werden, müssen im Auswahlfeld für Referenztag unter **Karteneigenschaften > Referenzeinheiten** aktiviert werden (siehe **Abbildung 22**). Dieses Kalibrierverfahren wird für TDoA beschrieben.

Abbildung 23: Referenz-Tag-Eigenschaften



MAC Address:	00	0C	CC	5E	63	A3
Coordinates:	X 6.07	Y -4.75	Z 1			



Single-Click-Aufzeichnung - Eine bevorzugte Methode für die Kalibrierung ist der Single-Click-Aufzeichnungsvorgang. Damit wird eine oder mehrere Gruppen von Tags definiert und für einen kurzen vordefinierten Zeitraum auf der Karte platziert. Eine Aufzeichnung wird initiiert, und die erfassten Daten werden basierend auf Timestamp und Map Identification direkt auf der MSE gespeichert.

Die besten Ergebnisse werden erzielt, wenn die Referenzgruppe von Tags in kompakter Reihenfolge auf einem kleinen Würfel oder einem Mast angeordnet ist. Dieselbe Gruppe kann neu positioniert werden, und die Prozedur wiederholt sich mehrmals auf derselben Karte, wenn Sie die Gruppe neu positionieren und die Aufzeichnung mit einem Mausklick neu starten. Alternativ können mehrere Gruppen auf derselben Karte definiert und in einer Sequenz aufgezeichnet werden.

Abbildung 24: Tools von AeroScout Systems Manager

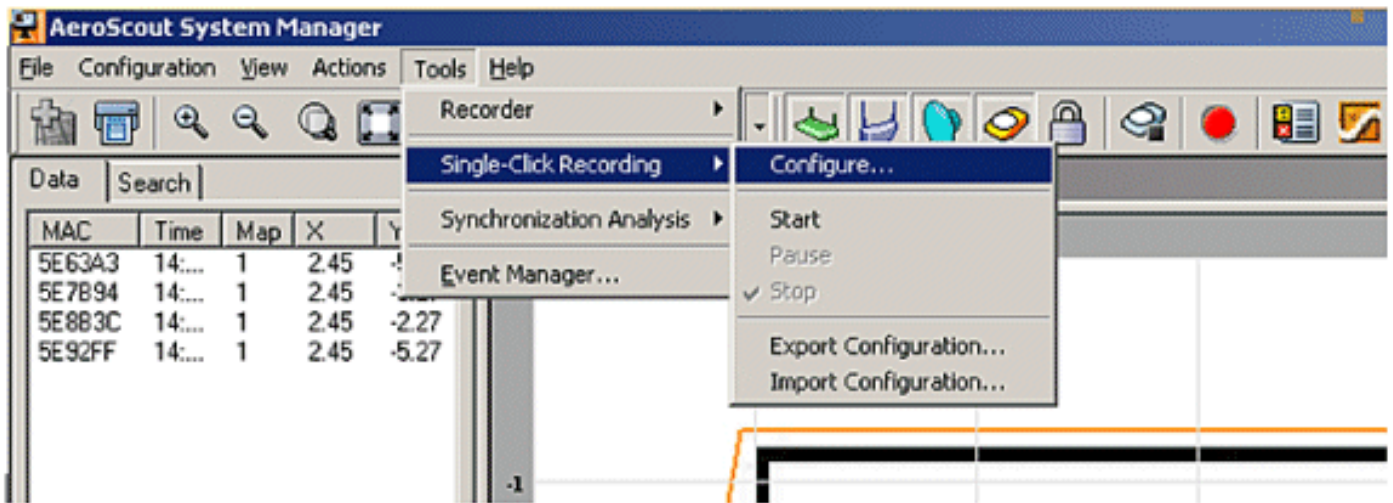
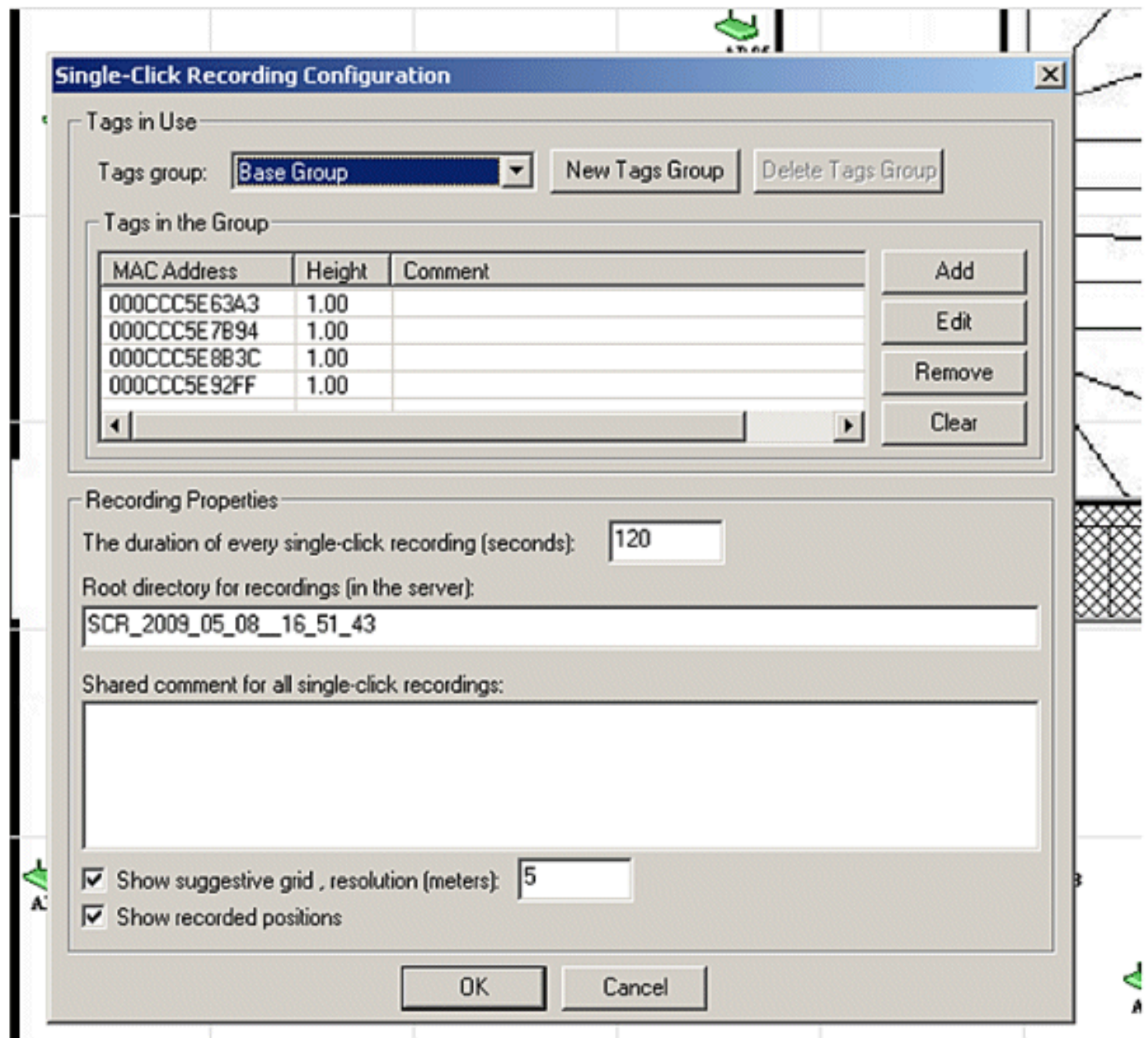


Abbildung 25: Konfiguration der Aufzeichnung per Mausklick



Geben Sie zur Durchführung dieser Methode die Konfigurationsinformationen unter **Extras > Single-Click Recording (Einzelklick-Aufzeichnung in den Abbildungen 24 und 25)** ein. Die Aufzeichnungseigenschaften können geändert werden, wenn die Standardwerte nicht geeignet sind. Die Aufzeichnungen werden automatisch in Unterverzeichnissen gespeichert, basierend auf

dem Zeitpunkt und dem Datum der Aufzeichnung.

Analyzer Tool - Bevor die Einzelklick-Aufzeichnungsdaten für die Kalibrierung verwendet werden können, müssen sie angezeigt und in eine Mesh-Datei konvertiert werden. Mit dem System Manager müssen die auf der MSE gespeicherten aufgezeichneten Datendateien in das System exportiert werden, in dem das Analysetool verwendet werden kann, um die aufgezeichneten Daten anzuzeigen und gegebenenfalls zu ändern, bevor eine Mesh-Datei erstellt wird. Die resultierende Mesh-Datei wird zurück in die MSE importiert, wo sie auf die Zuordnungseigenschaften angewendet werden kann, wenn Sie das RSSI Location Calculation Mesh zusammen mit der Upload-Dateiauswahl auswählen.

Eine ausführliche Erklärung finden Sie in der [AeroScout-Dokumentation](#) für weitere Konfigurationsinformationen und den Kalibrierprozess.

Weitere Informationen finden Sie in der [AeroScout-Dokumentation](#) zur AeroScout Mesh-Dateigenerierung.

[Exciter \(Chokepoint Trigger\)-Technologie](#)

Bei diesen Geräten handelt es sich um Geräte für die Proximity-Kommunikation, die Asset-Tags auslösen, um ihr Verhalten zu verändern, wenn ein Asset-Tag in die Nähe eines Aufregers gelangt. Diese Änderung kann dazu führen, dass das RFID-Tag seine eindeutige Kennung übermittelt oder dass das Tag seine interne Konfiguration oder seinen internen Status ändert. Eine der Hauptfunktionen eines Chokepoint-Triggers besteht darin, die Asset-Tags so zu stimulieren, dass sie der MSE anzeigen, dass das Tag in einen bestimmten Bereich eingedrungen oder aus diesem entfernt wurde. Auswahlpunkte sind Eingangs- oder Ausgangspunkte, die den Durchgang zwischen verbundenen Regionen ermöglichen. Häufige Schokoladenpunkte sind Türen, Korridore und Treppen. Zu den Standorten von Chokepoints im Innenbereich gehören angeschlossene Ein- und Ausgänge.

Exziter verwenden keine Triangulation und benötigen daher keine Signale, die von mindestens drei APs erkannt werden müssen.

Auslöser können Verhaltensänderungen in Tags auslösen, die das Standortsystem sofort darüber informieren, dass die markierte Ressource in den Chokepoint-Bereich eingedrungen oder aus diesem entfernt wurde. Die RFID-Tags übertragen dann die Identität des Chokepoint-Triggers an die Cisco UWN-Infrastruktur. Die im Tag-Paket enthaltenen Chokepoint-Informationen liefern der MSE Informationen zum Überschreiben von RF-Fingerprinting-Standortkoordinaten und zum Übernehmen der Checkpoint-Position für eine bestimmte Dauer.

Best Practices für die Konfiguration und Abstimmung von Begrüßern und Tags finden Sie im Konfigurationshandbuch von Exiter und Tag in der [AeroScout-Dokumentation](#).

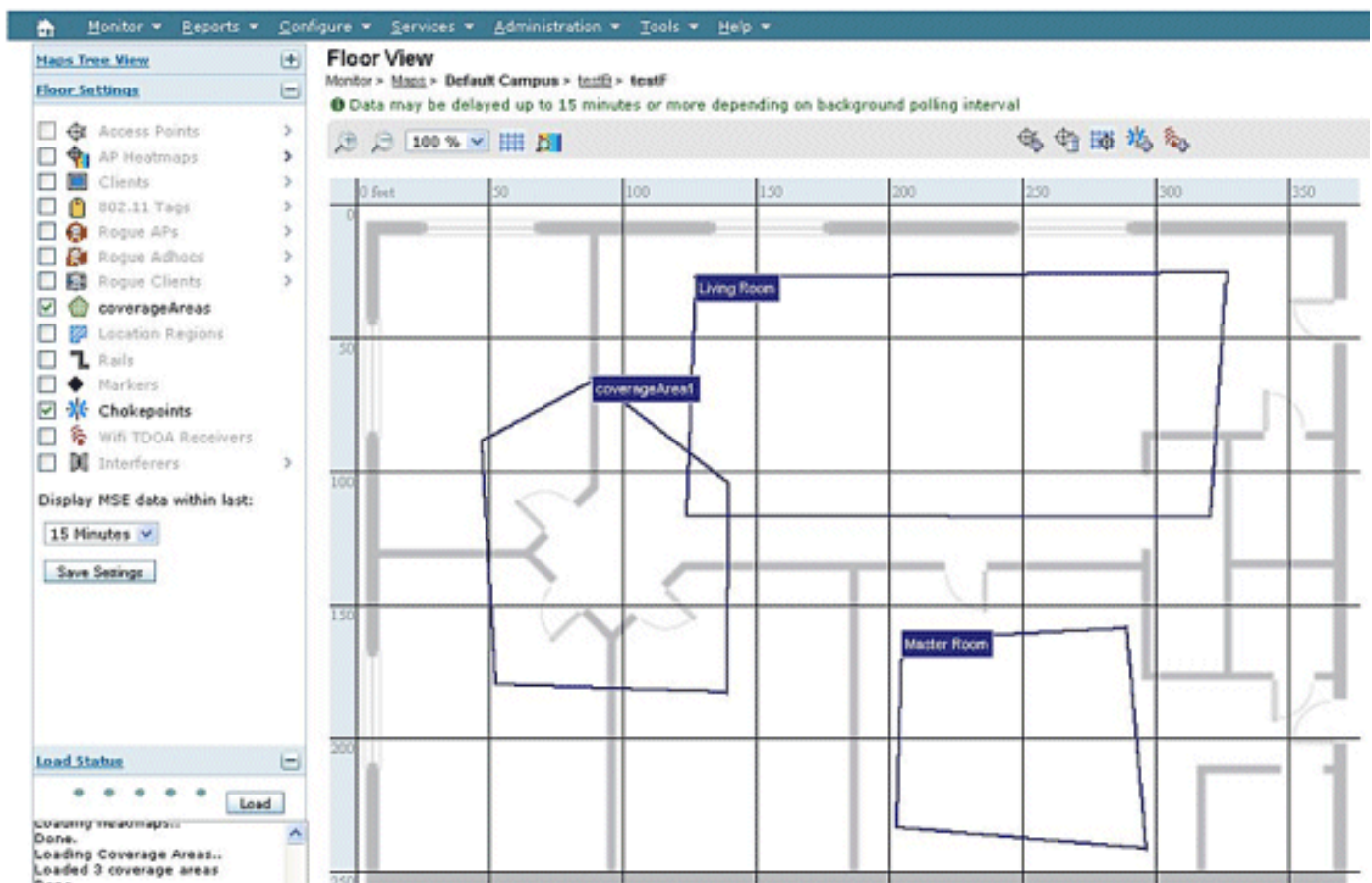
[Überlegungen zur Bereitstellung kontextsensitiver Informationen mit vorhandenen Daten- und Sprachdiensten](#)

In Kundenbüros, in denen bereits Wireless-Netzwerke vorhanden sind, müssen Sie die Implementierung der Context Aware Mobility Solution überarbeiten, um die Genauigkeit und potenzielle Abdeckungslücken zu ermitteln. Dabei handelt es sich um allgemeine Leitlinien:

- Maximaler effektiver Abstand zwischen den Access Points in den meisten standortbasierten Umgebungen: 12 bis 21 Meter

- Mindestens 3 APs im Übertragungsbereich jedes Clients (empfehlen 4 APs für Redundanz)
- Platzieren Sie Perimeter-APs zuerst, da Access Points die gewünschten Bereiche der Standortabdeckung umschließen müssen.
- Next-Place-APs zur Minimierung von Abdeckungslücken bei mindestens -75 dBm
- Im quadrilateralen Bereich müssen an den vier Ecken des Bereichs mindestens 4 APs installiert sein.
- Faktoren, die die Genauigkeit beeinflussen: AP-Platzierung, Wandmaterialien, große bewegliche Objekte und HF-Interferenzen
- Möglicherweise muss die Bodenfläche in Unterbereiche aufgeteilt und Unterbereiche unabhängig entworfen werden, um große Hindernisse zu berücksichtigen, die HF-Signale behindern (siehe **Abbildung 26**). Es werden bis zu 50 Abdeckungsbereiche für den Boden unterstützt. Die Größe der Abdeckungsfläche darf nicht kleiner sein als der typische Standortbereich (~10 m).

Abbildung 26: Map Editor in WCS stellt mehrere Abdeckungsbereiche bereit



- APs werden vorzugsweise entlang und innerhalb des Perimeters eines geschlossenen Bereichs positioniert.
- APs müssen gleichmäßig verteilt werden, d. h. APs müssen relativ weit voneinander entfernt sein.
- Die physische Platzierung von APs darf nicht zweiseitig erfolgen, selbst wenn sie in gleichen Entfernungen voneinander aufgestellt werden.
- Verwenden Sie das Location Readiness Tool in WCS, um die Effektivität der Gesamtbodenabdeckung zu messen.
- Durch die Verteilung von APs gebildete geometrische Formen beeinflussen die Genauigkeit: Die Anordnung des gleichseitigen Dreiecks bietet eine höhere Genauigkeit als

APs, die ein obskures Dreieck bilden. Die Platzierung auf einem Quadratmeter bietet bessere Ergebnisse als Access Points, die Rechtecke bilden.

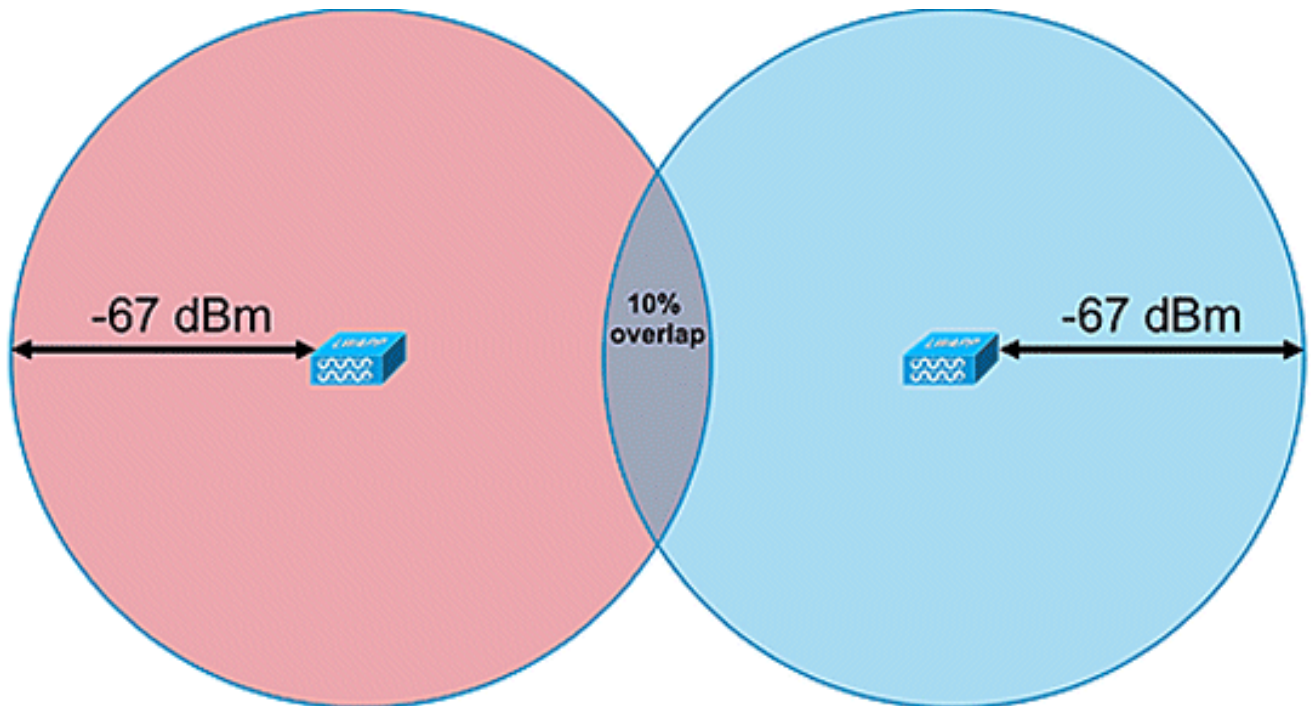
Abbildung 27 veranschaulicht das Konzept der Zellüberschneidung für ein Cisco 7921G VoWLAN-Mobilteil mit 802.11bg. Für den Cisco 7921G wird im Designleitfaden für Voice Over Wireless LAN empfohlen, dass die Überlappung zwischen den Zellen bei Verwendung von 802.11bg etwa 20 % und bei Verwendung von 802.11a ca. 15 % betragen sollte.

Datenanwendungen weisen nicht dieselbe Empfindlichkeit gegenüber Paketverlusten auf wie Sprachanwendungen. Daher ist nicht der gleiche Grad an Zellen-zu-Zelle-Überlappung erforderlich wie bei VoWLAN-Bereitstellungen. In den meisten Fällen reicht eine mindestens 10 %-ige Überlappung zwischen Zellen für ein zuverlässiges Roaming mit Datenanwendungen aus, wie in **Abbildung 28** gezeigt. Hochgeschwindigkeits-Datenanwendungen und Anwendungen, die Sprach- und Datenfunktionen in einem Gerät (z. B. Smartphones) kombinieren, erfordern möglicherweise eine Überlappung zwischen den Zellen, die einem VoWLAN-Design weit mehr ähnelt als ein Datendesign.

Abbildung 27: Zellenübergreifende Überlappung - Bereitstellung von Sprache und Daten (20 % Zellenüberlappung)



Abbildung 28: Inter-Cell Overlap - Datenbereitstellung (10 %-Zellen-Overlap)



Allgemeine Richtlinien - TDOA

Bei TDOA-basierter Bereitstellung sind mindestens drei Empfänger erforderlich, aber vier Empfänger liefern genauere Ergebnisse. Dies sind die allgemeinen Regeln für die TDOA-Empfängerdichte:

- Außenbereich: Die durchschnittliche Dichte beträgt einen TDOA-Empfänger pro 20.000 bis 50.000 m². (1.900 - 4.700 m²).
- Große Innenbereiche - die durchschnittliche Dichte beträgt einen TDOA-Empfänger pro 5.000 bis 14.000 m². (450 - 1.300 m²).
- Der Abstand zwischen synchronisierten Quell- und TDOA-Empfängern beträgt bei Bereitstellungen im Außenbereich maximal 150 m.
- Die Entfernung zwischen synchronisierten Quell- und TDOA-Empfängern beträgt bei großen Installationen in Innenräumen maximal 70 m.

Zwei wichtige Überlegungen für TDOA: Die Bereitstellung der Receiver-Dichte hängt von der Receiver-Synchronisierung und der Rx-Empfindlichkeit der Funkabdeckung der verfolgten Geräte ab. Der zweite wichtige Gesichtspunkt besteht darin, über eine ausreichende Abdeckung der Standortempfänger zu verfügen, um eine Empfangsdichte von mindestens drei Standortempfängern an jedem Punkt im Bereich sicherzustellen.

In bestimmten Szenarien müssen große Bereiche in Unterbereiche unterteilt werden. Wenn beispielsweise ein großes Lagerhaus durch eine Wand abgetrennt ist, muss es als zwei Unterbereiche ausgelegt werden. Die besten Ergebnisse werden erzielt, wenn die Sichtlinie zwischen der Synchronisierungsquelle und den Wi-Fi-TDOA-Empfängern beibehalten wird.

Dies sind zusätzliche Richtlinien für die Platzierung von Wi-Fi-TDOA-Empfängern:

- TDOA-Empfänger für Wi-Fi müssen sich am äußeren Perimeter befinden und gleichmäßig verteilt sein.
- Zusätzliche Wi-Fi TDOA-Empfänger können innerhalb der Grenze der Perimeterempfänger benötigt werden, abhängig von der Größe des Bereichs.
- TDOA-Empfänger müssen gleichmäßig verteilt sein und ein gleichseitiges Dreieck bilden

(wenn drei Wi-Fi-TDOA-Empfänger verwendet werden) oder Polygon (vier oder mehr Wi-Fi-TDOA-Empfänger).

Verwenden Sie in Bezug auf Wi-Fi TDOA-Receiver-Antennen Diversity-Antennen, um Multipath-Probleme zu beheben. Wi-Fi-TDOA-Empfänger, die sich am Perimeter des abgedeckten Bereichs befinden, müssen Richtantennen enthalten, um die Rezeption nur im abgedeckten Bereich zu konzentrieren. Verwenden Sie in der Ecke eines Perimeters eine 90-Grad-Richtungsantenne, und verwenden Sie entlang des Perimeters Richtantennen mit 180-Grad-Ausrichtung.

Omnidirektionale Antennen müssen mit im Perimeter befindlichen Wi-Fi-TDOA-Empfängern verwendet werden. Empfangsantennen müssen sowohl auf die Synchronisierungsquelle (vorzugsweise Sichtlinie) als auch auf den betreffenden Bereich zeigen.

Antennen müssen in Bereichen aufgestellt werden, in denen sie nicht durch Hindernisse wie Betonwände, große metallische Objekte oder dicht bedeckte Baumflächen behindert werden. Sie müssen so gut wie möglich (möglichst) in den überdachten Bereich eingebaut werden. Die bevorzugte Montagehöhe liegt 3 bis 5 m über der Oberfläche des verfolgten Geräts. Ist dies aufgrund der Umgebung nicht möglich, muss das Abdeckungsmuster, d. h. das Höhenmuster - typische Antennen haben eine Höhe von ca. 35 Grad, entsprechend angepasst werden. Entlang des Perimeters müssen Antennen an hohen Stellen in Richtung Abdeckungsbereich geneigt werden (bis zu 30 Grad nach unten), um die Höhe auszugleichen.

Weitere Informationen finden Sie im *AeroScout TDOA Deployment Guide*.

Kabelgebundener Standort

Mit der Softwareversion 6.0 können sowohl kabelgebundene als auch Wireless-Geräte mit der Context Aware-Lösung verfolgt werden. Mit kabelgebundenen Standorten bietet die MSE Funktionen zum Erfassen und Verwalten von CIVIC-Standortinformationen für Switches und Switch-Ports. Sie können den Standort von kabelgebundenen Ethernet-Geräten identifizieren, die mit einem dieser Cisco Switches verbunden sind: Stackable Catalyst Switches (Switches der Serien 3750, 3750-E, 3560, 2960 und IE-3000) oder Switch-Blades (3110, 3120, 3130, 3040, 30 und 3020) und Catalyst 4K-Serie (WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515 WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E und WS-X45-SUP6 LE). Verwenden Sie für kabelgebundene Standorte die folgenden IOS-Versionen, die sich auf das jeweilige Switch-Modell beziehen: IOS 12.2 (50)SE für Catalyst 3K-Switches und IOS 12.2(52)SG für Catalyst 4K-Switches. Die Informationen zum kabelgebundenen Standort werden von diesen Switches über NMSP an die MSE gesendet.

Standortinformationen werden über die IOS-CLI auf dem Cisco Switch konfiguriert. Kabelgebundene Switches werden im WCS definiert und mit einer MSE synchronisiert. Details zu kabelgebundenen Clients werden von einem standortfähigen Switch über eine NMSP-Verbindung an die MSE gesendet. Mit Cisco WCS können Sie dann kabelgebundene Switches und kabelgebundene Clients anzeigen.

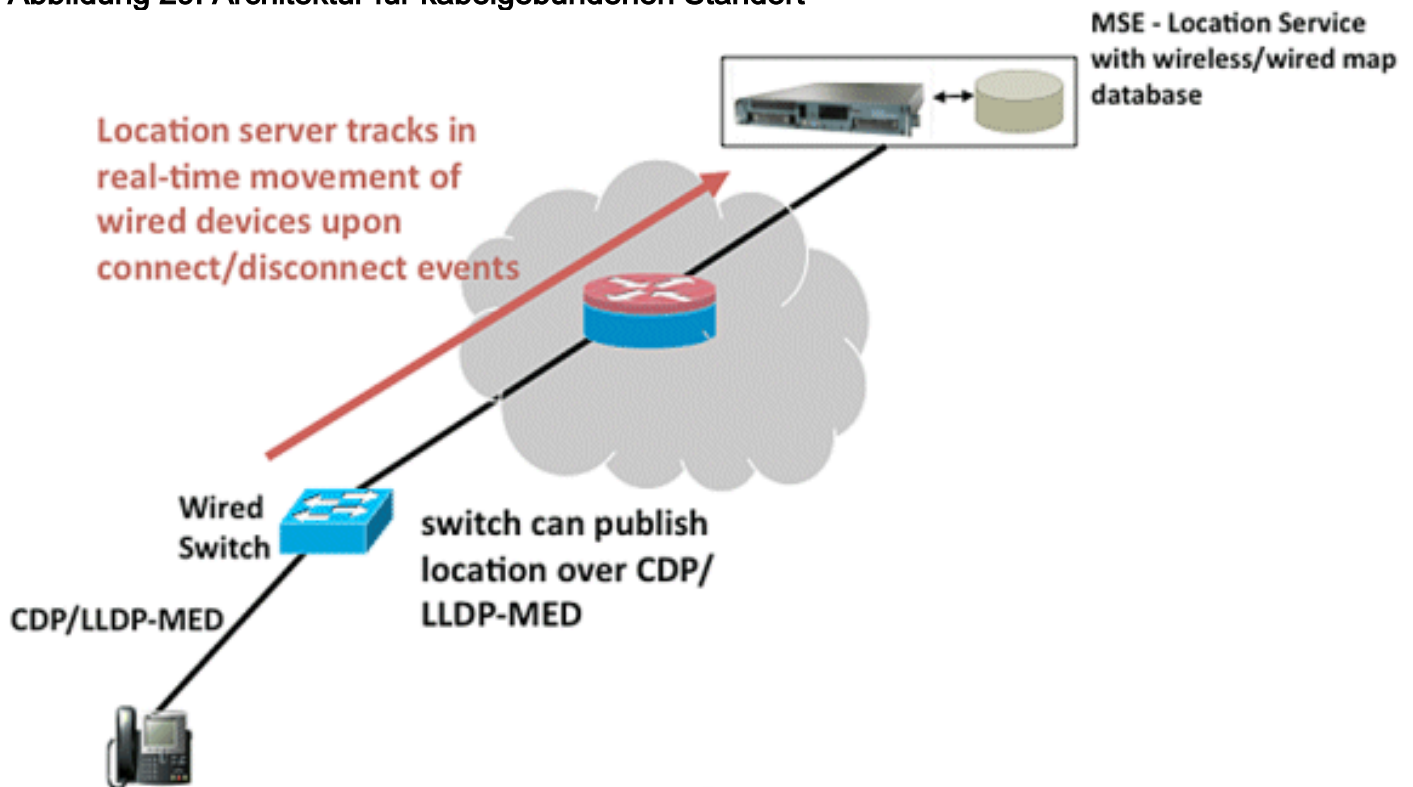
Die Import- und Anzeige von Informationen zum öffentlichen und Notfall-Standort (ELIN) entspricht den Spezifikationen von RFC 4776, die unter <http://tools.ietf.org/html/rfc4776#section-3.4> aufgeführt sind.

Die MSE verfolgt nicht nur den Standortverlauf der kabelgebundenen Clients, sondern stellt auch die SOAP/XML-APIs für externe Systeme bereit, die am Standort von Chassis oder Endgeräten interessiert sind, oder sucht/verfolgt einen Client in kabelgebundenen und Wireless-Kategorien. Siehe **Abbildung 29**.

- Switches übermitteln der MSE-Switch-Port-Zuordnung verbundene Geräte, die Standort- und UDI-Informationen des Chassis sowie Linecards enthalten.
- Die MSE verfolgt aktiv Informationen und Standorte von Geräten und Chassis.

Hinweis: Die Funktion für kabelgebundene Standorte bietet derzeit keine Möglichkeit, kabelgebundene Clients auf Bodenkarten zu suchen oder visuell anzuzeigen.

Abbildung 29: Architektur für kabelgebundenen Standort



Befolgen Sie die Schritte, um den kabelgebundenen Standort anzuzeigen.

Dies sind die Konfigurationsschritte auf der Switch-Seite:

1. Kenntnis der Steckplatz-/Modul-/Port-Konfiguration (1/0/20)
2. Verwenden Sie die richtige IOS-Version, die sich auf das jeweilige Switch-Modell bezieht: IOS 12.2 (50)SE für Catalyst 3K-Switches und IOS 12.2(52)SG für Catalyst 4K-Switches.
3. Aktivieren Sie den NMSP.
4. Aktivieren Sie die IP-Geräteverfolgung.
5. Konfigurieren Sie die SNMP-Community mit Lese- und Schreibzugriff.
6. Konfigurieren Sie die City/ELIN-Standortidentifikatoren.
7. Weisen Sie den Switch-Schnittstellen Bezeichner zu.

Dies sind die Konfigurationsschritte auf dem WCS:

1. Gehen Sie zu **Konfigurieren > Ethernet-Switches**.
2. Hinzufügen von Ethernet-Switches Fügen Sie die IP-Adresse hinzu. **Standortfähig** aktivieren. Geben Sie die SNMP-Community ein (Lese- und Schreibzugriff). Der eingegebene SNMP Community String muss mit dem dem Catalyst Switch zugewiesenen Wert übereinstimmen.
3. Gehen Sie zu **Services > Services synchronisieren > Switches**. Klicken Sie auf **Zuweisen**, um sie der bevorzugten MSE zuzuweisen. Wählen Sie den Switch aus, und synchronisieren Sie ihn.

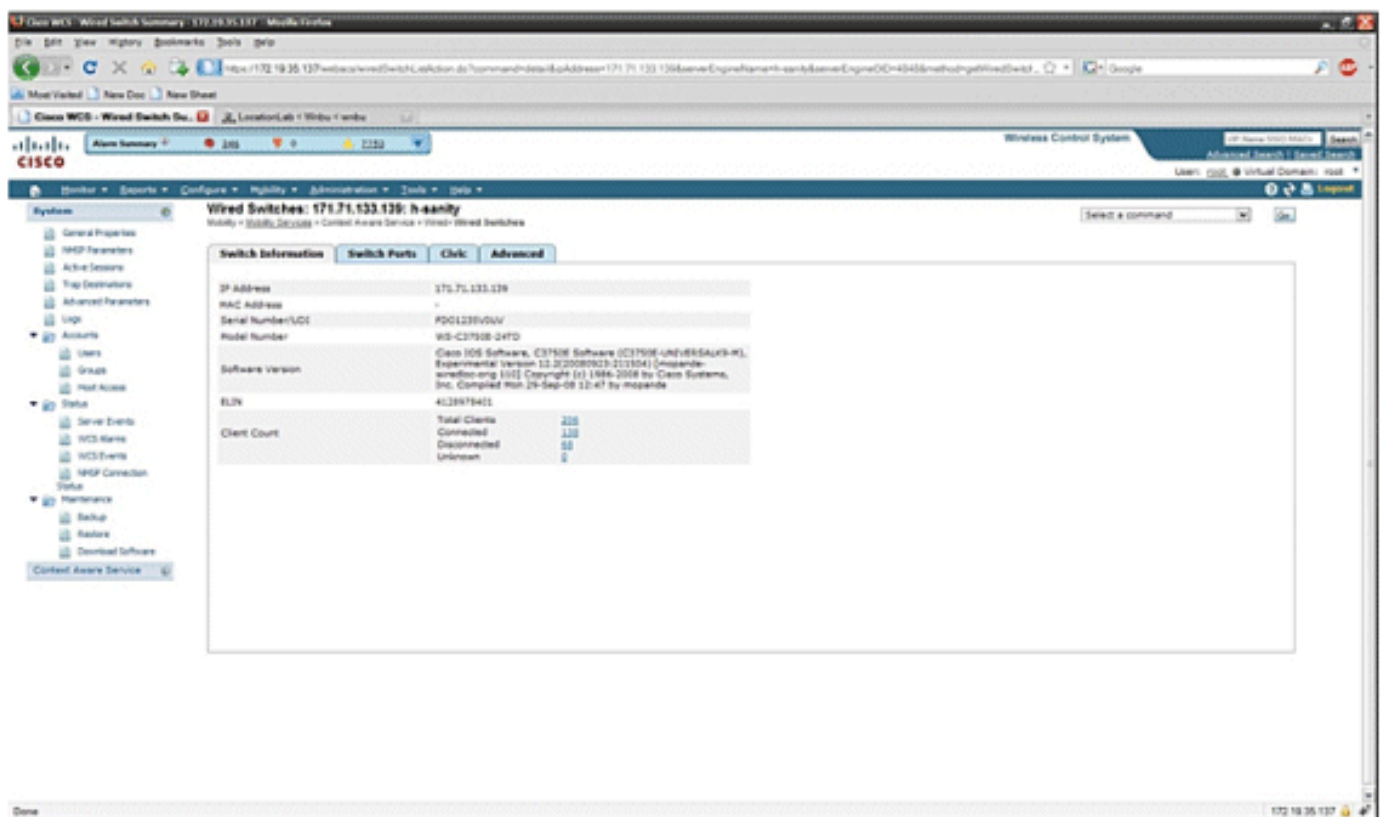
- Gehen Sie zu **Services > Mobility Services**, und klicken Sie auf **MSE**. Gehen Sie zu **System > Status > NMSP Connection status**. Überprüfen Sie, ob der aktive NMSP-Status für jeden Switch vorhanden ist.

Wenn Sie die Schritte für den Switch und das WCS abgeschlossen haben, können Sie die kabelgebundenen Elemente im WCS anzeigen:

- Klicken Sie unter Context Aware Services unter Wired auf **Wired Switches**.
- Eine Liste der Switches wird angezeigt.
- Klicken Sie auf **IP-Adresse des Switches**, um Details anzuzeigen (siehe **Abbildung 30**).

Hinweis: Zum Hinzufügen von WLCs zum WCS ist ein SNMP-Lese-Schreibzugriff erforderlich. Der WLC empfängt den MSE-Schlüssel-Hash nicht mit dem schreibgeschützten SNMP-Zugriffsmodus.

Abbildung 30: Kabelgebundene Switches - Switch-Informationen



- Sie können auch Switch-Ports und Bürgerinformationen anzeigen (siehe **Abbildung 31 bis 33**) oder die Listingreihenfolge (aufsteigend, absteigend) von Port-IP-Adressen, Steckplatznummern, Modulnummer und Portnummer ändern. Klicken Sie einfach auf die entsprechende Spaltenüberschrift.

Abbildung 31: Kabelgebundene Switches - Informationen zu Switch-Ports

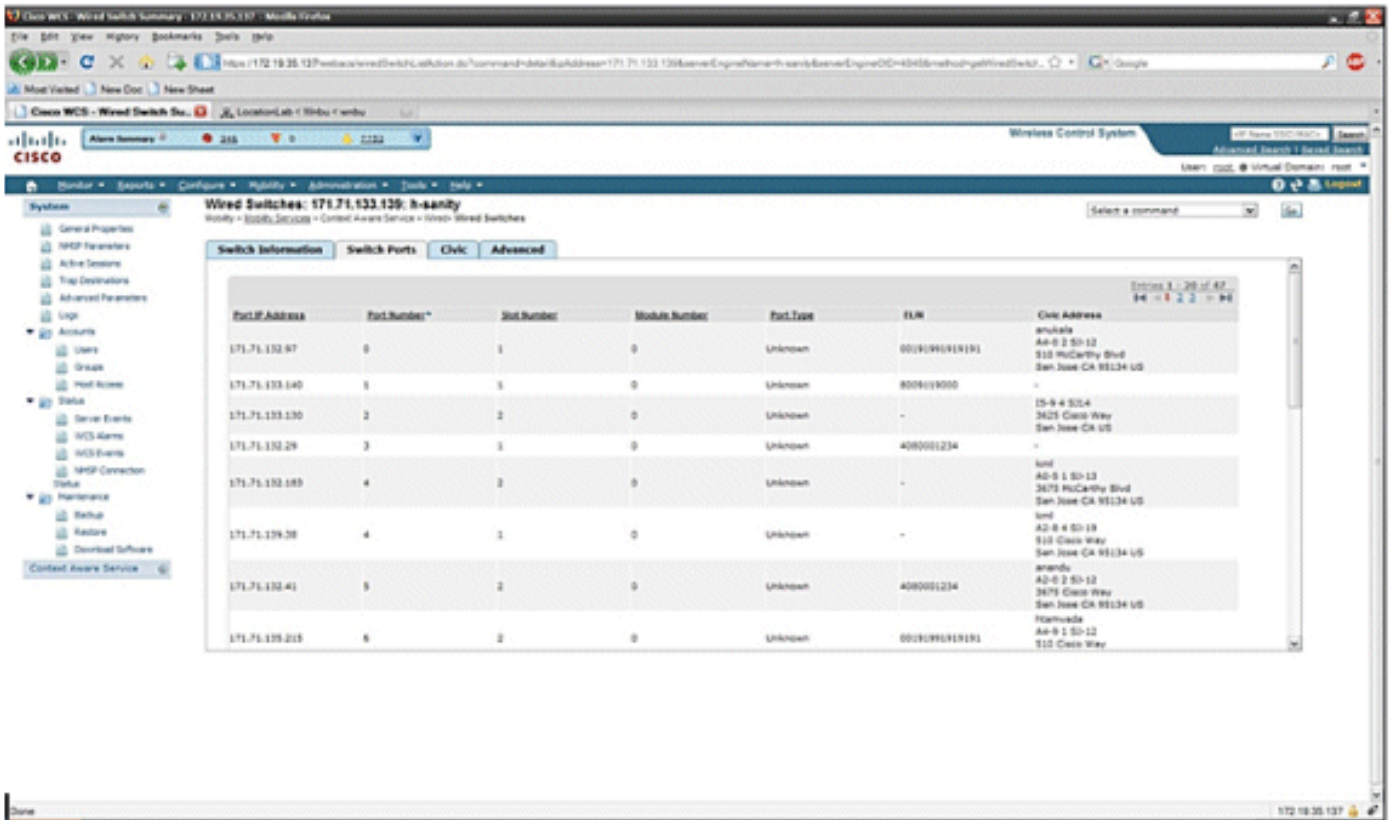
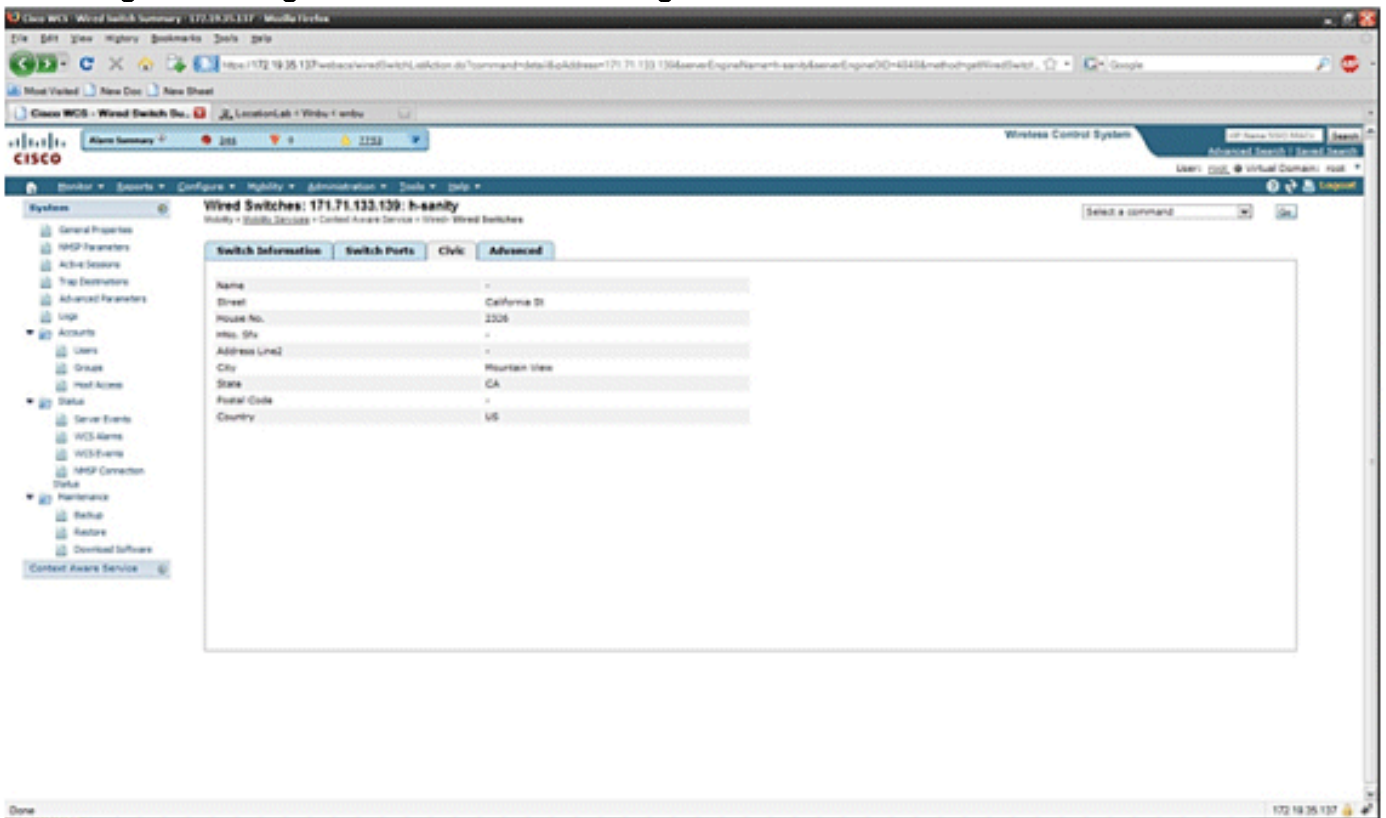
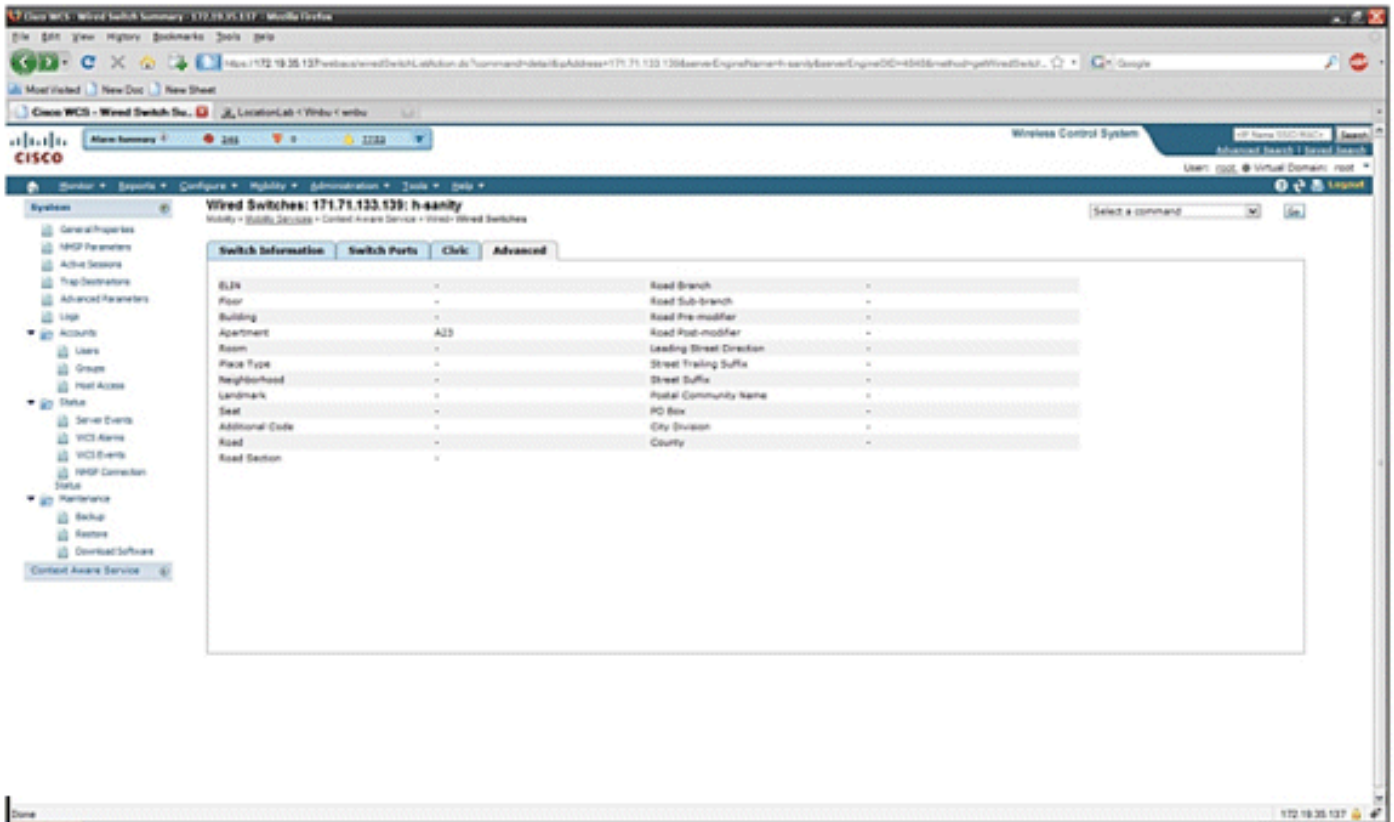


Abbildung 32: Kabelgebundene Switches - Bürgerinformationen



Die Registerkarte "Advance" enthält zusätzliche Bürgerinformationen:

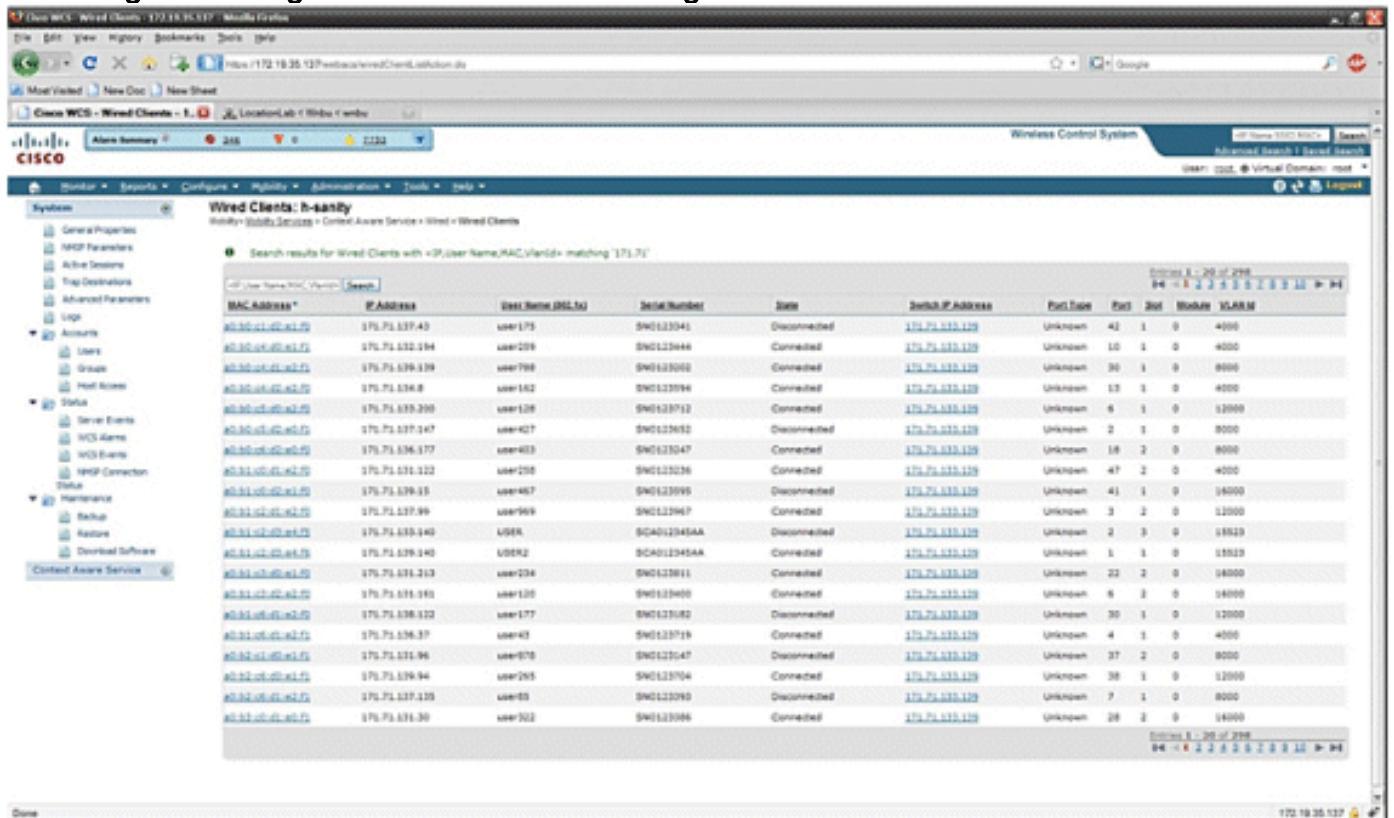
Abbildung 33: Kabelgebundene Switches - Erweiterte Informationen



Kabelgebundene Clients, die von allen Switches angezeigt werden, können angezeigt werden, wenn Sie unter **Wired Context Aware Service > Wired > Wired Clients** auf **Wired Clients** klicken.

Kabelgebundene Clients können nach IP-Adresse/partieller IP-Adresse/MAC-Adresse/partieller MAC-Adresse/802.1x-Benutzername/VLAN-ID durchsucht werden, wie in **Abbildung 34** gezeigt.

Abbildung 34: Kabelgebundene Clients - Suchergebnisse



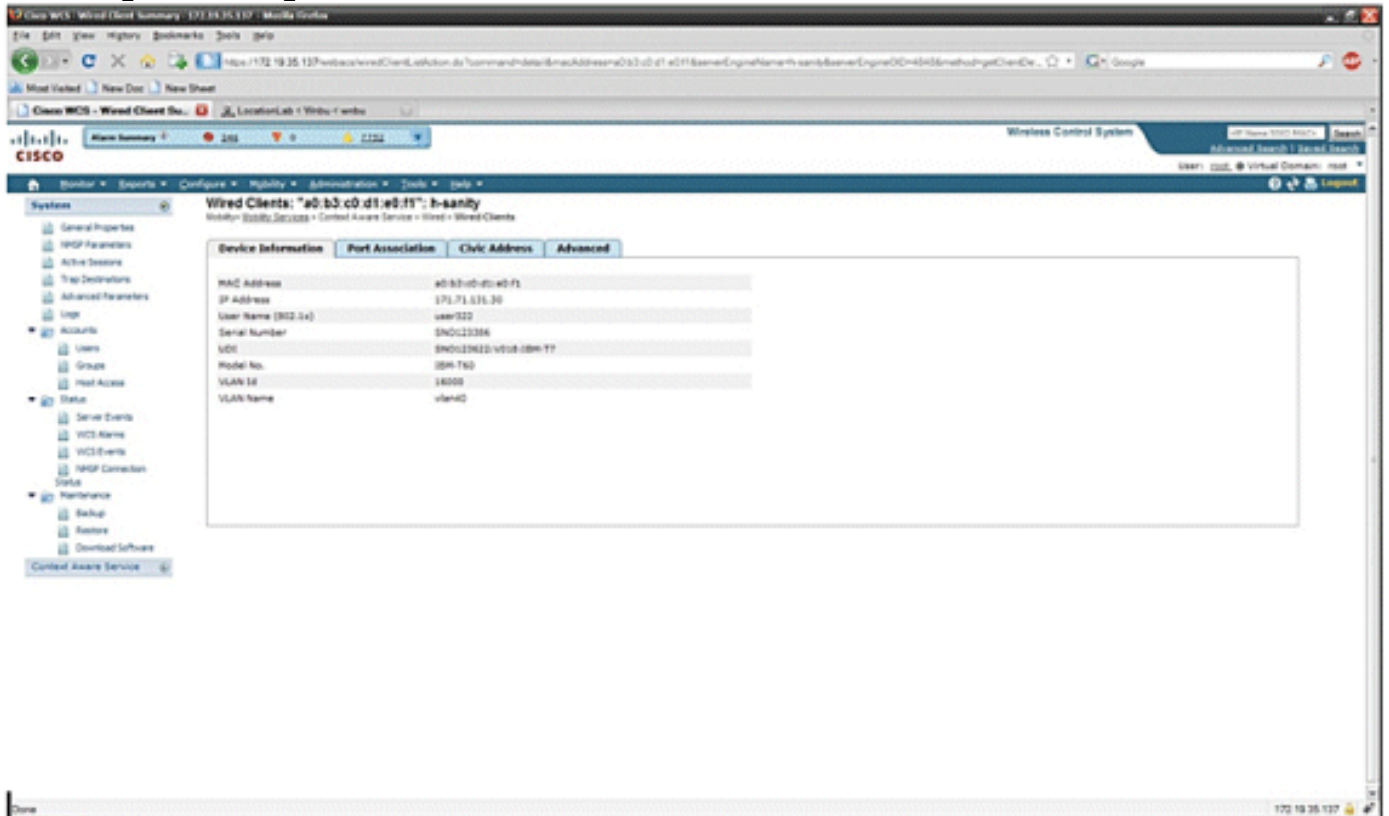
Ein Switch verfügt über eine angegebene Anzahl von Switch-Ports und -Clients. Hosts sind an

diesen Ports verbunden. Wenn Sie den Standort für einen bestimmten Switch-Port konfigurieren, wird davon ausgegangen, dass der an diesem Port verbundene Client den Port-Standort hat.

Wenn ein Switch (Switch2) mit einem Port (z. B. Port1) an einem anderen Switch (Switch1) verbunden ist, werden allen mit Switch2 verbundenen Clients der Ort zugewiesen, der auf Port 1 konfiguriert ist.

Sie können auch Details zu kabelgebundenen Clients anzeigen, wenn Sie auf den entsprechenden Client klicken, um Geräteinformationen, Port-Zuordnungen, Bürgeradressen usw. abzurufen (siehe **Abbildungen 35 bis 38**).

Abbildung 35: Kabelgebundene Clients - Geräteinformationen



Klicken Sie auf die Registerkarte Port Association (Portzuweisung), um die physische Position des Switch-Ports/Steckplatzes/Moduls anzuzeigen, auf dem der verkabelte Client terminiert, den Client-Status (verbunden, getrennt oder unbekannt) und die IP-Adresse des Switches:

Abbildung 36: Kabelgebundene Clients - Informationen zur Port-Zuordnung

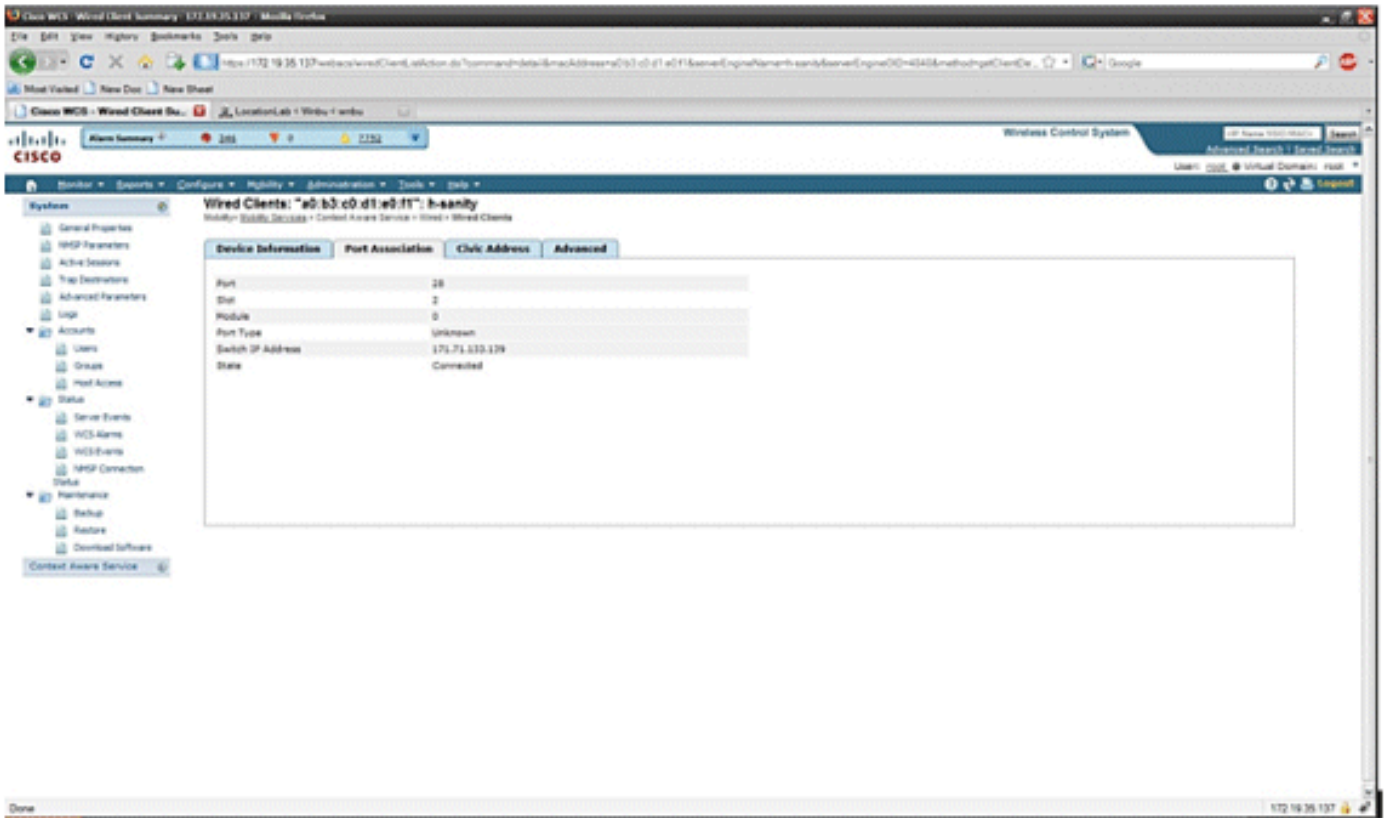


Abbildung 37: Kabelgebundene Clients - Informationen zu privaten Adressen

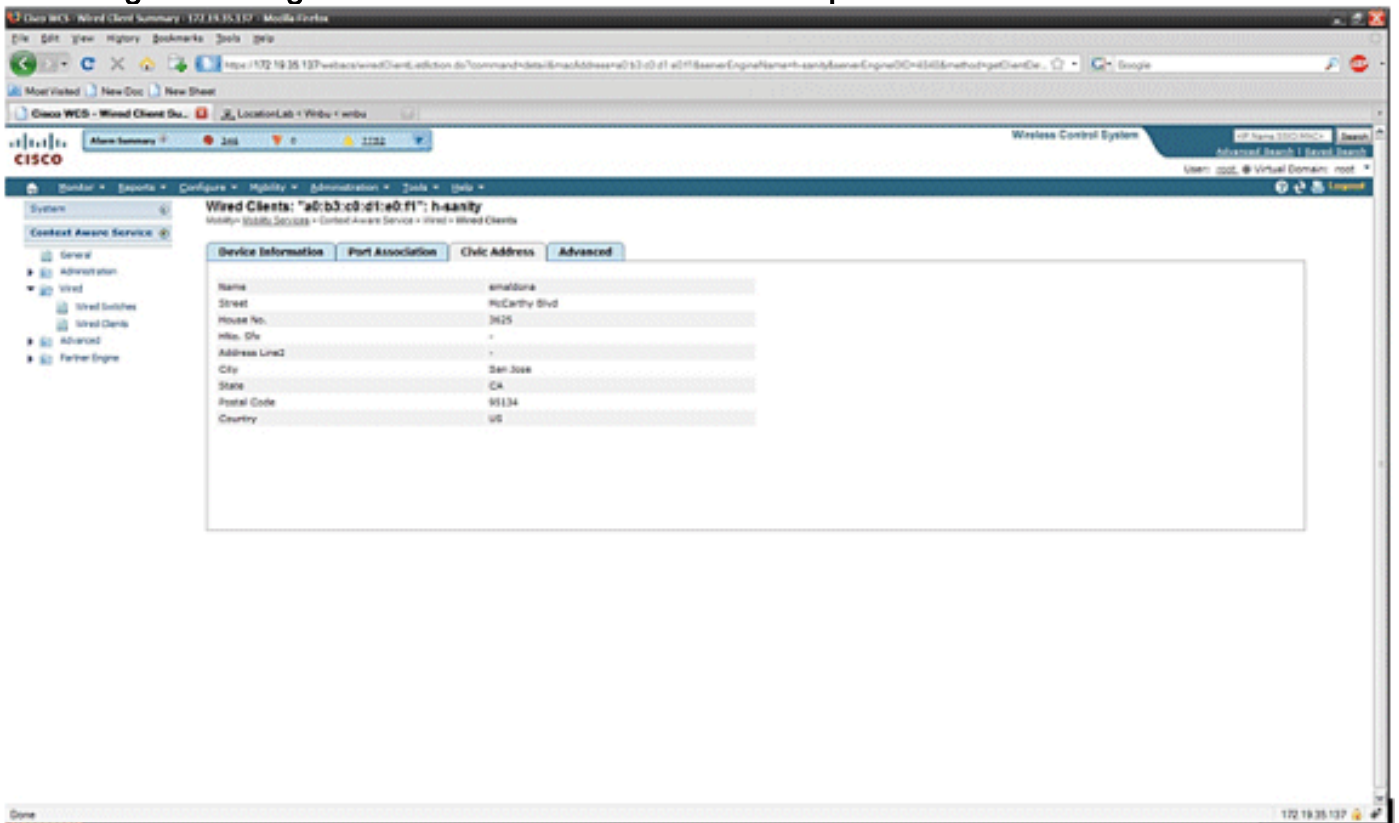
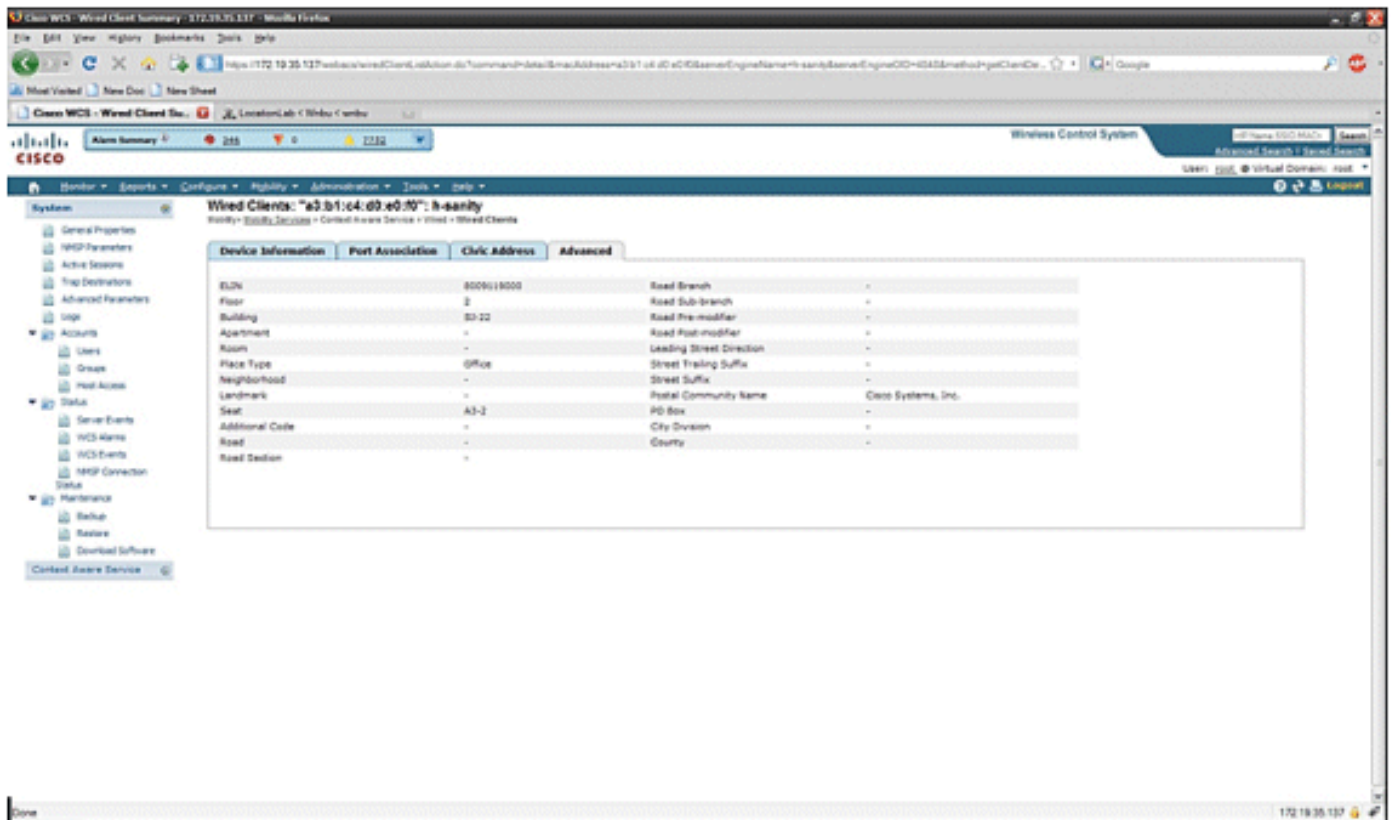


Abbildung 38: Kabelgebundene Clients - Erweiterte Informationen



[Abschnitt 3: Validierung und Verbesserung Ihres kontextsensitiven Netzwerks](#)

[WCS Accuracy Tool](#)

Vor der Version WCS 5.0 war es für Benutzer schwierig zu wissen, welche Genauigkeit sie in ihrem Wireless-Netzwerk sahen. Es gab keine Standardmethode, um den Genauigkeitsgrad bei der Bereitstellung von Context Aware zu quantifizieren. Mit der Version WCS 5.0 wurde ein integriertes Genauigkeitstool eingeführt. Tag- und/oder Wi-Fi-Clients sind an Referenzpunkten auf der Fußbodenübersicht in WCS positioniert. Ein detaillierter Bericht wird von WCS erstellt, der unterschiedliche Genauigkeit und Fehlerverteilung über Zeit und Raum bietet.

Es gibt zwei Arten von Genauigkeitstests:

- Geplante Genauigkeit
- Bedarfsgerechte Bereitstellung

Die Benutzer können eine dieser Methoden auswählen, nachdem sie die Messfläche für die Durchführung des Genauigkeitstests gemäß **Abbildung 39** ausgewählt haben. Diese Tests werden auf demselben Boden ausgeführt.

Abbildung 39: Bedarfsgerechter Test

Position Test Points for Test 'test'

Tools > Location Accuracy Tool > On Demand Accuracy Test > Position Test Points for Test 'test'



Planmäßiger Genauigkeitstest: Dieser Test wird in einer aktiven Umgebung (Live-Netzwerk) ausgeführt. Clients und/oder Tags sind am Boden vorpositioniert, und der Test wird über WCS geplant. Bei diesem Test wird die "tatsächliche" Position eines Elements im Vergleich zur "gemessenen" Position verwendet. Der Benutzer kann den Test ändern:

- Hinzufügen/Löschen von Elementen
- Ändern der Positionen
- Zeitpläne ändern

Der Test kann als geplante Aufgabe ausgeführt werden und Alarme generieren, wenn er unter einen bestimmten Genauigkeitsbereich fällt. Dieser Testtyp muss regelmäßig ausgeführt werden, da sich die Funkumgebung in einer bestimmten Bereitstellung ändern kann. Dies wirkt sich wiederum auf die Genauigkeit des Standorts aus.

Abbildung 40: Genauigkeitstestergebnis

Accuracy Test Result (%)

98.14

Error Range (Meters)	% of Total
3.00 or less	49.31
3.01 to 5.00	25.86
5.01 to 7.00	17.53
7.01 to 10.00	5.11
10.01 or more	1.86

Im Beispiel in **Abbildung 40** repräsentieren 98,14 % die Anzahl der Geräte, die innerhalb von 10 m erkannt wurden, d. h. die Summe von 49,31, 25,86, 17,53 und 5,11.

Bedarfsgerechter Test: Dieser Test wird ausgeführt, wenn ein Benutzer keine aktiven Clients und/oder Tags in seinem Netzwerk bereitstellt und daran interessiert ist, die Genauigkeit zu messen. Dieser Test kann ausgeführt werden, wenn ein Fußboden keine vorpositionierten Tags/Clients aufweist. Dies ähnelt dem Genauigkeitstest, der in WCS vor Version 5.0 mit einem einzigen Client durchgeführt wurde. Der Benutzer platziert einen Client an einem bestimmten Standort und gibt diesen Standort in der Fußbodenübersicht in WCS an, indem er den Test mit "Drag & Drop" zieht. Der Benutzer klickt auf **Start**, wartet einige Minuten, bis der RSSI-Auflistungsprozess abgeschlossen ist, und klickt auf die **Stopp**-Schaltfläche. Der Benutzer kann dann den Test fortsetzen und zum nächsten Punkt auf der Fußbodenkarte übergehen. Wenn alle Punkte gesammelt wurden, kann der Benutzer auf die Schaltfläche **Ergebnisse analysieren** klicken, um den Test auszuführen. Dadurch werden die Genauigkeit der Ergebnisse in einem Berichtsformat ermittelt.

Dies sind die wichtigsten Punkte, die Sie beim Ausführen einer der folgenden Genauigkeitstests beachten sollten:

- Der Client muss von mindestens drei APs erkannt werden.
- Genauigkeit hängt von der Triangulation und dem RF-Fingerprinting ab
- **Erweitertes Debuggen** auf der MSE muss aktiviert sein.
- Warten Sie an einem bestimmten Punkt auf der Fußbodenkarte etwa eine Minute, bis der Kunde in Position ist, d. h. stationär, bevor Sie den Genauigkeitstest durchführen. Dadurch

erhält der Wireless-Client genügend Zeit, um die MSE mit ihrem Speicherort zu aktualisieren. Führen Sie den Test zwei Minuten lang aus.

Tool zur Standortbereitschaft

WCS bietet ein Tool - die Funktion "Inspect Location Readiness" (Standortbereitschaft für Inspektion), mit dem ein Netzwerkdesigner eine schnelle vorausschauende Prüfung der Standortleistung für einen Boden durchführen kann, bevor das Kabel gezogen, Geräte bereitgestellt oder Kalibrierungen durchgeführt werden.

Dieses Tool ist ein entfernungs-basiertes Vorhersagewerkzeug und geht von einem typischen Bürogebäude aus. Infolgedessen kommt es zu gewissen Abweichungen zwischen den prognostizierten und den tatsächlichen Ergebnissen. Cisco empfiehlt, das Tool zur Standortbereitschaft zusammen mit anderen Best Practice-Techniken zu verwenden.

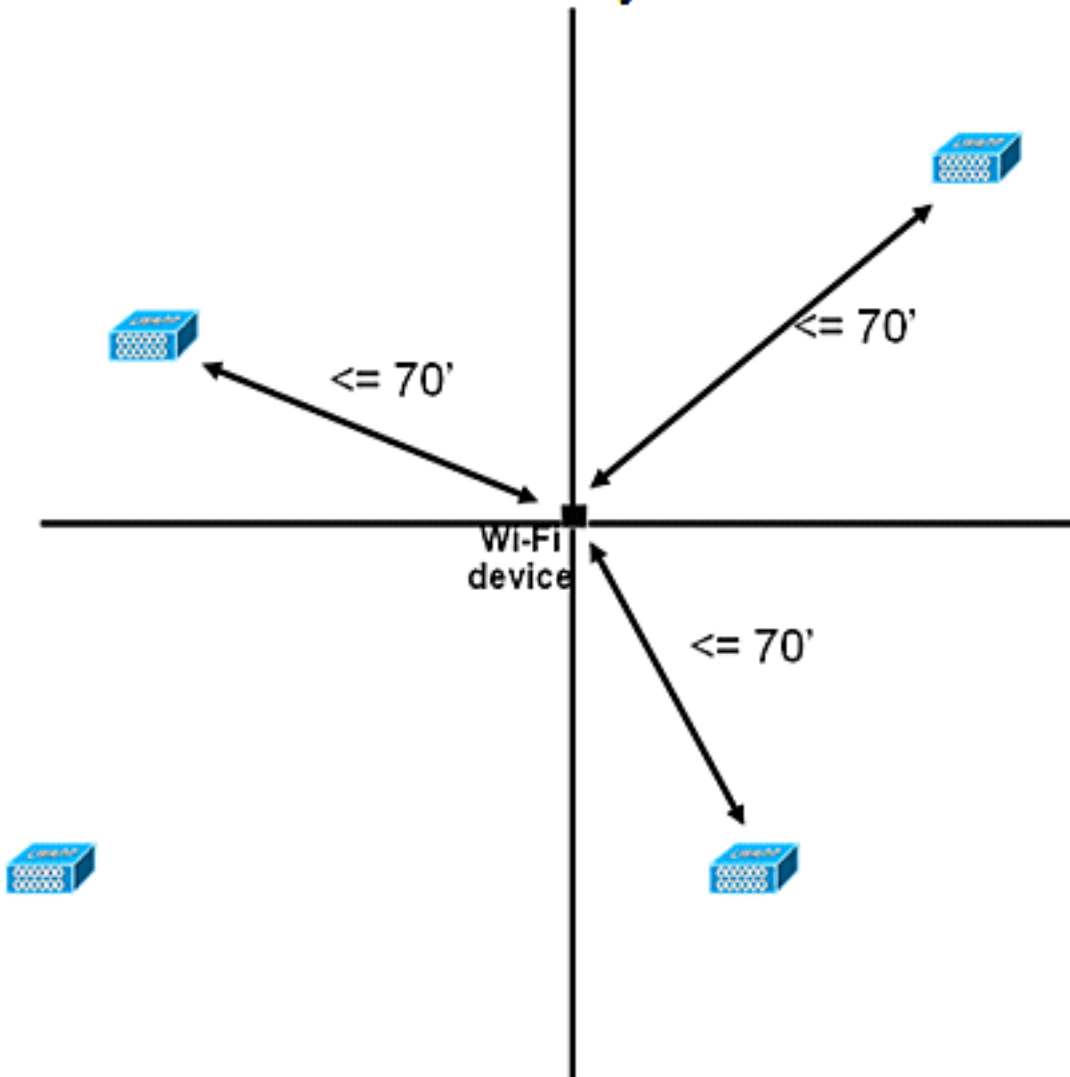
Bei der Eignung für den Prüfstandort wird die Platzierung der einzelnen Access Points zusammen mit dem Abstand zwischen den Access Points, der auf den Bodenkarten angegeben ist, berücksichtigt, um vorherzusagen, ob die geschätzte Genauigkeit der Standortverfolgung in 90 Prozent aller Fälle 10 Meter betragen wird. Die Ergebnisse der Überprüfung der Standortbereitschaft sind eine grüne und rote grafische Darstellung der Bereiche, die voraussichtlich diese Genauigkeit bzw. Problembereiche ergeben.

Das Location Readiness Tool setzt voraus, dass Access Points und Controller WCS bekannt sind und in den WCS-Bodenkarten definiert wurden. Wenngleich es nicht erforderlich ist, Access Points und Antennen an Wänden und Decken zu installieren, um die Standortbereitschaft zu beurteilen, müssen alle zutreffenden Controller zusammen mit den registrierten Access Points dem WCS hinzugefügt werden, wobei die Symbole die Access Points auf den entsprechenden Bodenkarten darstellen. Sobald die Access Points, die auf den Landkarten platziert werden sollen, der WCS-Datenbank hinzugefügt wurden, können mit diesen Access Points nachfolgende Analysen der Standortbereitschaft durchgeführt werden, auch wenn sie zu diesem Zeitpunkt nicht über WCS erreichbar sind. Da die Überprüfung der Standortbereitschaft auf der Platzierung der Access Points und den Entfernungen zwischen den Access Points auf den Karten auf den Etagen basiert, ist eine genaue Positionierung der Access Points bei Verwendung dieses Tools von entscheidender Bedeutung. Das Tool zur Standortbereitschaft dient lediglich dazu, die Eignung des Designs für die Durchführung der RF-Fingerprinting-basierten Standortverfolgung zu bewerten. Es überprüft keinen Aspekt des Designs, um die Position von Treffpunkten auszuführen, insbesondere nicht hinsichtlich der Definition oder Positionierung von Chokepoint-Triggern. Wählen Sie nach der Platzierung des Access Points die Bodenübersicht aus, für die Sie die Standortbereitschaft überprüfen möchten, und wählen Sie dann im oberen rechten Dropdown-Menü die Option **Inspect Location Readiness (Standortbereitschaft des Inspektors prüfen)** aus.

Ein Punkt wird als "standortbereit" definiert, wenn alle diese Kriterien erfüllt sind:

- Auf der Etage sind mindestens vier Access Points vorhanden.
 - Es wird festgestellt, dass sich in jedem Quadrant, der den betreffenden Punkt umgibt, mindestens ein Access Point befindet.
 - Mindestens ein Access Point befindet sich in jedem von mindestens drei umgebenden Quadranten, die sich innerhalb von 20 Metern vom betreffenden Punkt befinden.
- Abbildung 41** veranschaulicht diese drei Standortbereitschaftsregeln. **Abbildung 41: Standort-fähiger Punkt**

Definition of a "Location-Ready" Point



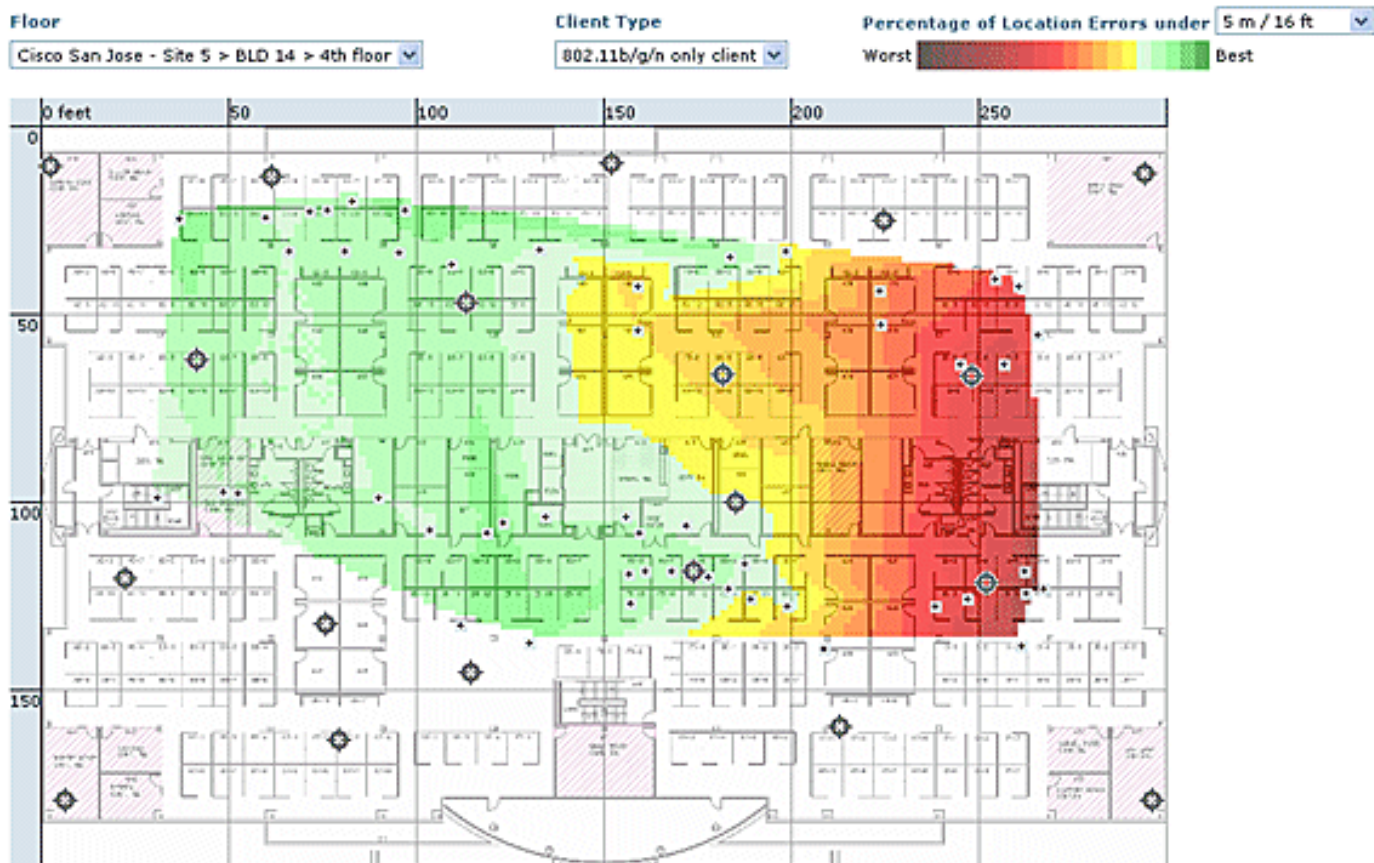
Die WCS-Bildschirmerfassung zeigt ein Beispiel für eine Bodenbereitstellung, bei der nicht alle Bereiche die zuvor beschriebene Drei-Punkte-Bewertung der Standortbereitschaft für eine Genauigkeit von 10 m/90 % bestanden haben. Obwohl es Grünflächen in der Mitte der Figur gibt, sollten Sie bemerken, dass rote Bereiche weit über die Perimeter-Access Points hinausragen, die den konvexen Rumpf darstellen. Mit einem fundierten Verständnis der Anforderungen, die die Standortbereitschaft definieren, können die in dieser Abbildung enthaltenen Informationen dazu verwendet werden, die Anzahl der Access Points zu bestimmen, die zur Leistungssteigerung neu platziert oder hinzugefügt werden müssen. Wenn beispielsweise in den roten Bereichen eine Genauigkeit von 10 m/90 % oder mehr erforderlich ist, können zusätzliche Access Points eingeführt werden, um einen klarer abgegrenzten Bodenperimeter zu erstellen, der die Platzierung von Access Points in den Ecken des Bodens beinhaltet und die Entfernungen zwischen Access Points erneut überprüft. Wenn Sie diese Änderungen implementieren, wird die Möglichkeit des Cisco UWN, den Standort von verfolgten Geräten in diesen hervorgehobenen Bereichen zu beheben, wahrscheinlich erheblich verbessert.

Abbildung 42: Beispiel für die Verwendung des Ortungsbereitschaftstools



Die Standortqualität kann für eine Wireless-Bereitstellung auf der Grundlage der Erfüllung der Standortspezifikation (10 m, 90 %) überprüft werden, die auf den Daten basiert, die im Rahmen einer physischen Prüfung und Kalibrierung gesammelt wurden (siehe **Abbildung 42**). Wenn Sie das Location Readiness-Tool verwenden, wird eine farblich gekennzeichnete Karte angezeigt, die Bereiche anzeigt, die den Spezifikationen für die 10-Meter-Position 90 % entsprechen (grün=Ja) und nicht entsprechen (rot=nein).

Abbildung 43: Tool für die Qualität des Prüforts



Nachdem Sie eine Kalibrierung für einen bestimmten Bereich oder eine bestimmte Karte durchgeführt haben, können diese Daten überprüft werden, um die während der Kalibrierung gesammelten Rohdaten zu überprüfen, wie in **Abbildung 43** gezeigt. Es ist wichtig, die Rohdaten an jedem Datenerhebungspunkt hinsichtlich der physischen Messung und des zugehörigen AP-RSSI-Werts zu überprüfen. Anomalien in der AP-Positionierung, der Antenne oder sogar in Messwerten können leicht identifiziert und korrigiert werden, bevor sie auf die Karten angewendet werden. Zusätzliche Informationen zum wahrgenommenen Genauigkeitsgrad und den beteiligten Zugangspunkten können ebenfalls dazu beitragen, die Genauigkeit des Gesamtstandorts zu bewerten.

Kontextsensitiv - Systemleistung

In einer bereitgestellten kontextsensitiven Lösung können mehrere Tags und/oder Clients gleichzeitig verschoben werden. Je mehr Geräte sich bewegen, desto größer ist die Verarbeitungslast für die MSE. Dies wiederum wirkt sich auf die Latenz des Netzwerks insgesamt aus. Latenz bezieht sich in diesem Kontext auf die Verzögerung zwischen dem Empfang von RSSI-Informationen über ein Gerät durch die MSE und dem Zeitpunkt, zu dem der Standort von der MSE berechnet wird. Dabei handelt es sich um die maximale Anzahl von Elementen, die sich jederzeit bewegen:

- 100 Elemente bewegen/Sekunde für MSE-3310
- 650 Elemente in Bewegung/Sekunde für MSE-3350

End-to-End-Latenz des Systems:

- Clients und Tags: zehn Sekunden bei voller Auslastung mit 650 bewegten Elementen/Sekunde (beginnt mit WLC Softwareversion 5.1)

Die Latenz bezieht sich auch auf das NMSP-Aggregationsfenster, das angepasst werden kann.

Weitere Informationen finden Sie im Abschnitt **"RFID-Tag und WLC-Konfiguration/-Optimierung"** im Unterabschnitt "Wie viel Zeit zwischen Iterationen?"

- Maximale Anzahl an Anwendungssitzungen: 1024
- Maximale Anzahl von Zielen für Northbound-API: 1024
- Maximale Anzahl Abdeckungsbereiche: 50/Stock Die Größe des Abdeckungsbereichs darf nicht kleiner sein als die typische Standortgenauigkeit (10 m). Die typische Abdeckungsgröße beträgt mindestens 15 x 15 m².

· **Anzahl APs pro Etage:**

MSE/2710 hat an sich keine Einschränkungen. Die Haupteinschränkung liegt in der Empfehlung von weniger als 100 APs gemäß WCS-Empfehlungen - andernfalls werden WCS-Karten nicht mehr zu verwalten, bieten eine schlechte Auflösung und sehr langsam erstellt Kartendetails. Außerdem ist die Anzahl der verfolgten Geräte, die auf einer WCS-Zuordnung angezeigt werden können, begrenzt.

· **Anzahl der Controller pro MSE:**

Derselbe Controller kann mit mehr als einer MSE synchronisiert werden, mit einigen Ausnahmen:

1. Wenn sich der Controller im Code 4.2 oder 5.0 befindet, werden mehrere NMSP-Verbindungen nicht unterstützt, sodass sie nicht mit mehr als einer MSE synchronisiert werden müssen.
2. WLC mit wIPS AP kann keine NMSP-Verbindung mit mehr als MSE herstellen. Dies liegt daran, dass der wIPS-AP nur mit einer MSE kommunizieren kann, die wIPS-Adaptive Services ausführt.

Ein WLC kann bis zu 10 NMSP-Verbindungen haben.

Eine MSE unterstützt bis zu 500 NMSP-Verbindungen. Dies muss jedoch aus der Perspektive der CAS-Bereitstellung verstanden werden. Jeder WLC kann mehrere Clients (5.000 Clients pro WLC4400) verfolgen. In pragmatischen Bereitstellungen mit sehr wenigen Controllern erreicht MSE CAS die Nachverfolgungsgrenze von bis zu 18.000 Geräten. Es gibt zwei Glasdecken, von denen eine zu bedenken ist, eine 5000 Clients pro Controller und die andere 18000 Geräte pro MSE 3350. Wenn wir eine dieser Grenzen erreichen, maximieren wir die Kapazität des Systems.

Skalierbarkeitstests sind in jedem Fall begrenzt. Wir haben Stresstests mit 100 Controllern pro MSE durchgeführt, auf denen Standortdatenverkehr läuft.

· **Anzahl der MSEs pro WCS:**

Obwohl MSE über ein WCS verwaltet werden kann, kann WCS mehrere MSEs verwalten. WCS hat aus verschiedenen Perspektiven Grenzen, die bestimmen könnten, wie viele MSEs es je nach Verteilung dieser Einheiten auf die MSEs verwalten könnte. Daher spielen Faktoren wie die maximale Anzahl unterstützter Elemente, die maximale Anzahl unterstützter Fußböden oder die maximale Anzahl unterstützter APs eine Rolle. Offiziell unterstützen wir 5 MSE pro WCS.

· **Anzahl der Netzwerkdesigns:**

Für die MSE wurden keine Einschränkungen für Netzwerkdesigns hinzugefügt. Allerdings hat Aeroscout Motor eine Grenze, abhängig von der Anzahl der Stockwerke, Abmessungen und Anzahl der Elemente für MSE. Die maximale Anzahl der Stockwerke ist auf 255 beschränkt. Wenn

Geräte alle 60 m bereitgestellt werden und die Grid-Auflösung 1 m beträgt, können kleine Installationen 15 Karten unterstützen und große Installationen (höhere Speicheranforderungen) 90 Karten unterstützen.

Northbound-Benachrichtigungen

Die MSE kann alle bekannten Tag-Daten an einen Northbound-SOAP-Listener weiterleiten. Wenn diese Konfiguration konfiguriert ist, kann die MSE den Listener jedes Mal benachrichtigen, wenn der Tag-Benachrichtigungsrahmen der MSE gemeldet wird oder wenn die MSE den Speicherort für ein Tag berechnet. Dies ist nützlich, wenn Anwendungen von Drittanbietern bei jedem Anhören eines Tags sofortige Updates erhalten möchten, anstatt diese regelmäßig abzufragen. Dies kann über die Benutzeroberfläche für Benachrichtigungsparameter konfiguriert werden: **Services > Mobility-Services > Context Aware Service > Advanced > Notification-Parameter**.

Befolgen Sie zur Unterstützung von Northbound-Benachrichtigungen die folgenden Empfehlungen:

- Reguläre Tag-Beacons dürfen nicht weniger als drei bis fünf Minuten voneinander entfernt sein.
- Das Tag-Benachrichtigungsintervall zum Verschieben von Tags muss zwischen einer und zehn Sekunden liegen.
- Der Warteschlangenlimit für Benachrichtigungsparameter muss größer als die Anzahl der unterstützten Tags sein.
- Stellen Sie sicher, dass der SOAP-Listener nicht ausfällt.
- Stellen Sie sicher, dass der SOAP-Listener als Antwort auf die Benachrichtigung einen gültigen leeren SOAP-Umschlag zurückgibt.
- Stellen Sie sicher, dass der SOAP-Listener die eingehenden Benachrichtigungen schnell verarbeitet.

Wenn diese Bedingungen nicht erfüllt sind, kann die Benachrichtigungswarteschlange der MSE einen Überlauf verursachen. Diese Bedingung wird auf der Seite "Notification Parameters" (Benachrichtigungsparameter) als Zähler "Notifications Dropped" (Benachrichtigungen verworfen) angezeigt (siehe **Abbildung 44**).

Abbildung 44: Northbound-Benachrichtigungen

- System
- Context Aware Service**
 - General
 - Administration
 - Wired
 - Advanced
 - Location Parameters
 - Notification Parameters**
 - Partner Engine
- wIPS Service

Notification Parameters: MSE4

Services > Mobility Services > Context Aware Service > Advanced > Notification Parameters

Northbound Notifications

Northbound Notifications Enable

Tags

Chokepoints

Telemetry

Emergency

Battery Level

Vendor Data

Include tag location information in notification

	IP Address	Port	Transport
Destination1	<input type="text"/>	<input type="text"/>	SOAP
Destination2	<input type="text"/>	<input type="text"/>	SOAP
Destination3	<input type="text"/>	<input type="text"/>	SOAP

Advanced

Rate Limit	<input type="text" value="0"/>	0 - 9999999 msec
Queue Limit	<input type="text" value="500"/>	1 - 99999
Retry Count	<input type="text" value="1"/>	0-60
Refresh Time	<input type="text" value="60"/>	0 - 99999 mins
Notifications Dropped	<input type="text" value="0"/>	

Dieser gesamte Abschnitt ist nur gültig, wenn der Northbound-Listener den Datenverkehr von Northbound-Benachrichtigungen nicht verarbeiten kann und diese unterdrücken möchte, es sei denn, der Tag hat etwas Wichtiges (oder von Interesse), um Folgendes zu melden:

Filtern von Northbound-Benachrichtigungen anhand von Tag-Payloads von Interesse, um das System besser skalierbar zu machen. Wenn beispielsweise alle paar Sekunden ein Tag-Beacon ausgibt, die Tag-Nutzlast jedoch nur Akkuinformationen oder Bewegungstelemetrie enthält, die nicht von Interesse ist, kann die Generierung von Northbound-Ereignissen beim Empfang dieser Tag-Payloads unterdrückt werden.

Die Northbound-Ereignisfilterung wird durch sechs neue Parameter in der Datei aes-config.xml gesteuert:

```
<entry key="send-event-on-location-calc">true</entry>
<entry key="send-event-on-every-beacon">true</entry>
<entry key="send-event-on-vendor">true</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
<entry key="send-event-on-telemetry">true</entry>
```

Um ALLE Benachrichtigungen zu erhalten, aktivieren Sie das Senden-Ereignis am Standort-Kalk und Senden-Ereignis-an-jedem-Beacon. Wenn nicht jede einzelne Tag-Payload von Bedeutung ist, legen Sie sie selektiv fest. Wenn die MSE beispielsweise Benachrichtigungen nur für eine Standortberechnung, einen Anrufknopfdruck oder ein Treffer auf einen Treffer senden soll, aktivieren Sie diese Option. (In der Datei auf "true" gesetzt. LÖSCHEN SIE DIESE WERTE NICHT!):

```
send-event-on-location-calc
send-event-on-emergency
send-event-on-chokepoint
```

Schalten Sie die anderen drei Markierungen aus.

```
After install/upgrade, ssh into MSE and issue the following commands :
rm /opt/mse/locserver/conf/aes-config.xml (won't exist for new install)
/etc/init.d/msed start (creates the aes-config.xml)
/etc/init.d/msed stop
vi /opt/mse/locserver/conf/aes-config.xml
```

Ändern Sie die Filter entsprechend Ihrer Anforderungen. Speichern Sie die Datei, und beenden Sie sie. Starten Sie den angefügten Prozess neu.

```
/etc/init.d/msed start
```

Weitere Informationen zur Benachrichtigung finden Sie im [API-Dokument](#).

[RFID-Tag und WLC-Konfiguration/-Optimierung](#)

Ein RFID-Tag ist ein Wi-Fi-Gerät, das mit einem Sender und einer Antenne ausgestattet ist. Da keine Verbindung zu Access Points hergestellt wird, verhält es sich nicht wie andere Wireless-Clients. Ein RFID-Tag überträgt Informationen in regelmäßigen Abständen, die als Tag-Benachrichtigungsrahmen bezeichnet werden. Hierbei handelt es sich um Multicast-Pakete, die mit niedrigen Datenraten versendet werden. Alle x Sekunden sendet das RFID-Tag den Frame der Tag-Benachrichtigung auf den konfigurierten Kanälen. Es wird empfohlen, Tag-Benachrichtigungs-Frames mit einer Signalstärke von 17 dBm zu übertragen. Wenn ein Zyklus über alle konfigurierten Kanäle hinweg abgeschlossen ist, befindet sich das RFID-Tag im Standby-Modus und wartet auf die nächste Übertragungszeit, um Tag-Benachrichtigungsrahmen zu übertragen.

Wenn Sie RFID für die Ressourcenverfolgung in Wi-Fi bereitstellen, muss dies konfiguriert werden:

1. Wie viele Tag-Benachrichtigungs-Frames pro Kanal werden vom RFID-Tag übertragen?

Aufgrund der Art des Multicast-Datenverkehrs in 802.11-Netzwerken ist es im Allgemeinen empfehlenswert, die Anzahl der Tag-Benachrichtigungs-Frames pro Kanal zu erhöhen.

In einer sauberen Funkumgebung empfangen APs Tag-Updates und melden diese an ihren WLC, selbst wenn das Tag so konfiguriert ist, dass ein Tag-Benachrichtigungsrahmen pro Kanal gesendet wird. Bei Bereitstellungen in der Praxis besteht eine hohe Wahrscheinlichkeit, dass ein Tag-Update bei einem bestimmten Access Point aufgrund von Funkstörung oder anderen

Aktivitäten verpasst wird. Wenn ein Tag-Update für einen nahe gelegenen Access Point fehlt, kann dies zu falschen Standortberechnungen führen. Wiederholen Sie die Anzahl der Tag-Benachrichtigungs-Frames pro Kanal auf zwei oder drei statt auf die Standardeinstellung, um die Wahrscheinlichkeit zu verringern, dass das Tag-Update von nahe gelegenen APs nicht gehört wird.

Die Berücksichtigung der Akkulaufzeit von Tags ist ebenfalls ein wichtiger Aspekt der Genauigkeit und des Tag-Benachrichtigungsintervalls. Oft ist eine Kompromittierung erforderlich. Best Practice-Empfehlungen zur Verfolgung beweglicher Objekte sind die Verwendung von Bewegungserkennungs-Tags. Konfigurieren Sie ein Tag-Benachrichtigungsintervall, d. h. 3 bis 5 Minuten bei stehendem Gerät, und verwenden Sie bei Bewegung ein verlängertes Frame-Intervall von 1 oder 2 Sekunden, um eine gute Genauigkeit zu erzielen und eine lange Akkulaufzeit zu ermöglichen. Die Konfiguration und Empfehlung für Best Practices finden Sie bei der Tagherstellung.

Weitere Informationen finden Sie in der [AeroScout-Dokumentation](#).

Eine weitere Möglichkeit, einen Tag-Update-Verlust für einen bestimmten Access Point auszugleichen, besteht in der Erhöhung des RFID-RSSI-Ablaufwerts auf dem WLC. Der empfohlene Wert muss das Dreifache des Intervalls + 5 Sekunden betragen. Mit diesem Wert wird der letzte RSSI auf dem WLC beibehalten, wenn ein WAP die letzte Iteration eines angegebenen Tags nicht erkennt. Neue Updates werden zusammen mit gespeicherten Daten aus früheren Iterationen an die MSE gesendet.

Ein Nachteil dieses Ansatzes ist, dass er die Genauigkeit beeinflussen kann. Wenn die Bewegungsübertragung auf einem RFID-Tag nicht aktiviert ist und sich das Tag schnell von dem letzten Ort entfernt, an dem es einen Tag-Benachrichtigungsrahmen übertragen hat, basiert die Standortberechnung auf den alten Daten. Es wird empfohlen, Motion Probing zu ermöglichen, die Standortberechnung stets auf frische AP-Daten zu stützen und die WLC-Timer so niedrig wie möglich zu halten, um die Latenz zu verringern.

Hinweis: Der WLC-Code 5.x bietet einen neuen Befehl, der sich auch auf die im WLC gespeicherten Daten auswirkt. Dieser Ablauftimer kann individuell für RFID-Tags, Clients und unberechtigte Benutzer konfiguriert werden. Die Standardeinstellung für das Ablaufdatum beträgt fünf Sekunden, bei der veraltete Daten vom Controller über einen Zeitraum von mehr als fünf Sekunden gelöscht werden. Die RFID-Timeout-Einstellung steuert die Gesamtdauer, die ein RFID-Tag auf dem Controller verbleibt, nachdem er aus der Reichweite gegangen ist oder die Übertragung beendet hat. Die Kombination dieser Timer mit zusätzlichen Einstellungen auf der MSE kann eine optimale Genauigkeit bei minimalen NMSP-Updates zwischen den Controllern und MSEs gewährleisten.

Das RFID-RSSI-Ablaufdatum kann mit der WLC-CLI konfiguriert werden:

```
(Cisco Controller) >config location expiry tags ?
```

```
<seconds>      Time in seconds
```

Dieser Befehl zeigt an, ob ein AP erkennt ein bestimmtes RFID-Tag ist:

```
(Cisco Controller) >show location ap-detect rfid ?
```

```
<AP name>      Display information for AP name
```

2. Welche Kanäle?

Bei einer Bereitstellung mit 2,4 GHz sind die Kanäle 1, 6 und 11 die nicht überlappenden Kanäle im Spektrum. Die für ein RFID-Tag zu konfigurierenden Kanäle sind 1, 6 und 11. Beachten Sie, dass ein AP in einigen Szenarien RFID-Tag-Updates auf einem anderen Kanal als dem, auf dem er ausgeführt wird, hören kann. Diese Updates werden vom Access Point standardmäßig verworfen und nicht an den WLC weitergeleitet.

3. Wie viel Zeit zwischen Iterationen?

Die Konfiguration des Tag-Benachrichtigungen-Frame-Intervalls spielt eine wichtige Rolle für die Standortverfolgung, da sie die Zeittrennung zwischen Standortberechnungen oder Updates definiert. Wie bereits erwähnt, muss das Tag-Benachrichtigungsintervall so konfiguriert werden, dass eine optimale Akkulaufzeit und Standortgenauigkeit erreicht wird, d. h. 3-5 Minuten bei stationären Tags.

Beachten Sie, dass beim Verschieben eines Tags mehr Echtzeitinformationen erforderlich sind, um den Speicherort zu berechnen. Bei der Verfolgung beweglicher Tags muss die Bewegungsübertragung auf dem RFID-Tag mit einem Tag-Benachrichtigungsintervall <10 Sekunden aktiviert werden.

4. Wie lange wartet ein RFID zwischen Frame-Übertragungen?

Beim Senden von Frames oder Beacons wartet ein Aeroscount-RFID-Tag eine vorkonfigurierte Zeitspanne zwischen den Übertragungen. Diese Wartezeit kann 128, 256 oder 512 Millisekunden betragen und wird als "Nachrichtenwiederholungsintervall" bezeichnet. Wenn 512 ms konfiguriert sind und das Tag pro Kanal ein Beacon sendet, schließt das RFID-Tag innerhalb von ca. 1,5 Sekunden eine vollständige Iteration ab. Wenn pro Kanal zwei Frames mit demselben "Wiederholungsintervall" gesendet werden, schließt das Tag innerhalb von 3 Sekunden eine vollständige Iteration ab.

Das RFID-Tag überträgt die konfigurierte Anzahl von Frames auf einem bestimmten Kanal und wechselt dann zum nächsten Kanal, um dieselbe Routine auszuführen. Die Zeit, die jede Frame-Übertragung trennt, wird als "Nachrichtenwiederholungsintervall" bezeichnet.

Der WLC muss Tag-Updates von allen beteiligten APs auf den Kanälen 1, 6 und 11 empfangen, bevor er diese Daten über NMSP an die MSE sendet. Der WLC wartet eine konfigurierbare Zeitspanne, das so genannte Aggregationsfenster, bevor er die nahe gelegene AP-Liste für ein RFID-Tag an die MSE sendet.

Ab der WLC 5.1-Software ist das NMSP Aggregation Window konfigurierbar und standardmäßig auf zwei Sekunden eingestellt. Bei Versionen vor 5.1 ist das Aggregationsfenster auf dem WLC acht Sekunden lang nicht konfigurierbar. Wenn ein Controller dasselbe Paket von mehreren APs im gleichen Aggregationsfenster empfängt, werden die Duplikate verworfen. Wenn ein Paket in einem Fenster eingeht und der Rest im nächsten, sendet es ein doppeltes Paket (das erste im zweiten Fenster), verwirft aber den Rest der Duplikate.

Es ist wichtig, die richtige Größe des Aggregationsfensters zu konfigurieren, um sicherzustellen, dass der WLC Updates von allen APs erhalten hat. Dieses Fenster muss größer sein als die Zeitdauer, die ein RFID-Tag für den Abschluss eines Zyklus verbringt. Die gängige Praxis besteht darin, mindestens eine zusätzliche Sekunde hinzuzufügen, um sicherzustellen, dass der WLC lange genug wartet. Die Konfiguration eines niedrigen Aggregationsfensters führt zu einer falschen Standortberechnung.

CCA (Clear Channel Assessment) kann zusätzliche Zeit für ein RFID-Tag bereitstellen, um alle

drei Channel-Updates abzuschließen. Die meisten RFID-Tags erkennen Trägersignale, bevor sie übertragen werden. Wenn das Wireless-Medium ausgelastet ist, wird es für zusätzliche Zeit abgeschaltet und die Übertragung wird unterlassen. Wenn das Medium frei ist, übertragen sie nach einer vordefinierten Zeit den nächsten Kanal. Wenn das Medium immer noch besetzt ist, unterbricht das Tag die Übertragung für diese Kanalwiederholung und wechselt zum nächsten Kanal. Die maximale Zeit für die Rückerstattung ist nicht festgelegt und kann von Anbieter zu Anbieter variieren.

Hinweis: Wenn Sie WLC 4.x- oder WLC 5.x-Softwareversionen zusammen mit der MSE verwenden, ist das NMSP-Aggregationsfenster auf der MSE auf 8 Sekunden festgelegt.

Konfiguration und Optimierung von WCS und MSE











Es gibt eine Reihe wichtiger Konfigurationsparameter, die in WCS und MSE konfiguriert werden können und die die Standortverfolgung beeinflussen können (siehe **Abbildung 45**).

Abbildung 45: Standortparameter

Location Parameters: MSEWCS4

Services > Mobility Services > Context Aware Service > Advanced > Location Parameters

Location Parameters

Enable calculation time 	<input type="checkbox"/> Enable
Enable OW Location 	<input type="checkbox"/> Enable
Relative discard RSSI time 	<input type="text" value="3"/> 1 - 99999 min
Absolute discard RSSI time 	<input type="text" value="60"/> 1 - 99999 min
RSSI Cutoff 	<input type="text" value="-75"/> -90 to -50 dBm
Enable Location Filtering 	<input checked="" type="checkbox"/> Enable
Chokepoint Usage 	<input checked="" type="checkbox"/> Enable
Use Chokepoints for Interfloor conflicts 	<input type="text" value="Never"/>
Chokepoint Out of Range Timeout 	<input type="text" value="60"/> 1-99999 secs
Absent Data cleanup interval 	<input type="text" value="1440"/> 1 - 99999 mins

Der RSSI Cutoff ist ein wichtiges Feld, das für eine bestimmte Umgebung eingestellt werden kann. Dieses Feld gibt den RSSI-Mindestwert an, unter dem die MSE beim Berechnen des Speicherorts für ein bestimmtes Element ignoriert. Dieser Wert gilt nur für die Verfolgung von Clients, d. h. nicht für die Tag-Verfolgung.

Wenn Sie einen sehr hohen RSSI-Cutoff angeben, z. B. -60 oder -50 mit niedriger AP-Dichte, führt dies zu einer schlechten Standortberechnung, da die MSE die RSSI-Werte zuverlässiger Hearing-

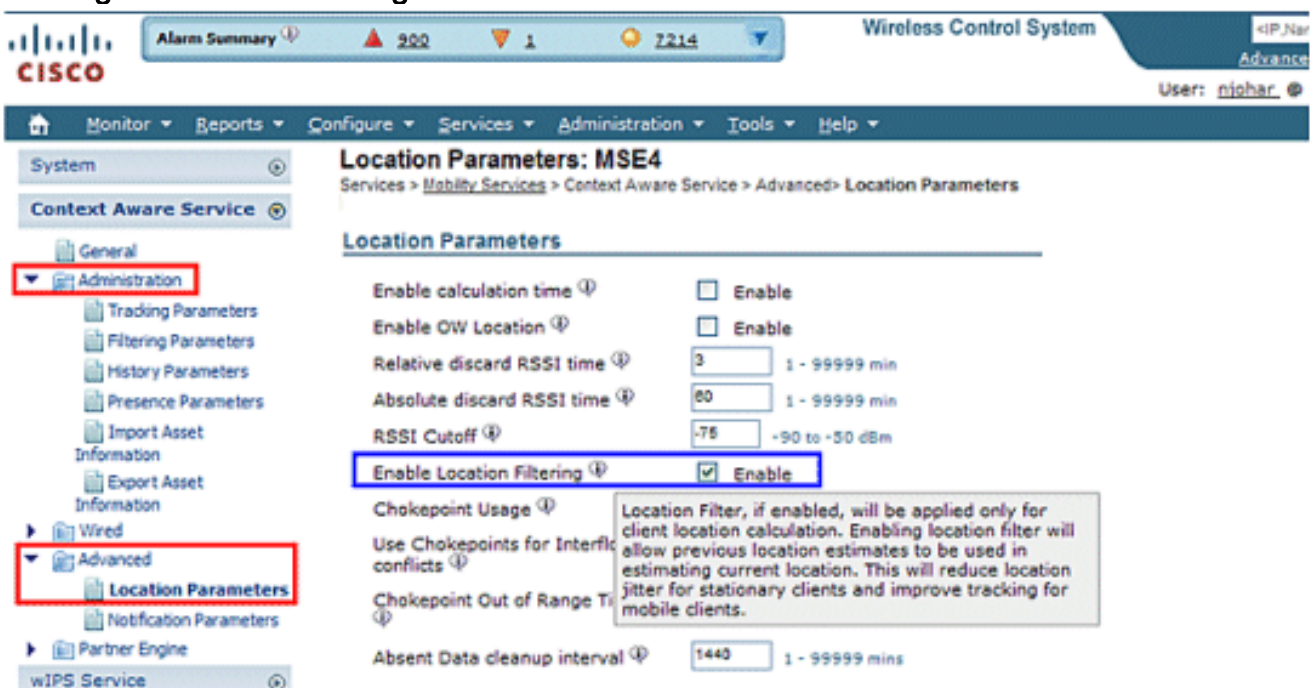
APs von ihrer Berechnung ausschließt.

Wenn Sie einen niedrigen RSSI-Cutoff verwenden, z. B. -85 von -90, und in einem freien Raum oder mit niedrigen Wänden arbeiten, führen Dämpfungsbereiche zwischen den Etagen zu einer schlechten Standortberechnung, da die MSE RSSI-Werte von den äußeren Access Points in die Berechnung einbezieht.

Obwohl der RSSI-Cutoff ein fester Wert ist, kompensiert der Algorithmus fehlende Werte, wenn er niedrigere RSSI-Werte von der letzten Iteration ergänzt oder Werte aus dem relativen Discard Repository annimmt. Im Idealfall ermöglicht der optimale RSSI Cutoff-Wert mehr als fünf dazu beitragende APs mit RSSI-Werten von mehr als -75 dBm im gleichen Stockwerk. Gebäude mit nicht charakteristischem HF-Verlust können eine Anpassung dieses Parameters erfordern, aber dies ist normalerweise ein Hinweis auf eine suboptimale Bereitstellung.

Jitter: Vor der Version 5.2 verfügte die MSE über einen Ortungsmechanismus, um Clients zu verfolgen. Der bewegliche Durchschnitt wurde für Clients ermittelt, d. h., die Bewegungen der Clients waren durchschnittlich. Ab Version 5.2 der Software wurde dieser gesamte Mechanismus durch "Standortfilter" ersetzt. Die Standortfilterung wird intern auf Client-Basis angewendet. MSE überwacht, welcher Client bewegt und welcher stationär ist, und wendet die Filterung entsprechend an. Dadurch wird der Jitter des Systems insgesamt verringert. Die Standortfilterung ist standardmäßig aktiviert. Siehe **Abbildung 46**.

Abbildung 46: Standortfilterung



WCS/MSE-Kommunikation: Dies ist die Bereitstellungsempfehlung zur Konfiguration der Kommunikation zwischen WCS und MSE:

- **MSE:** HTTPS ist immer aktiviert (standardmäßig). HTTP ist standardmäßig deaktiviert. Die Aktivierung von HTTP erfordert eine manuelle Konfiguration über den Konsolenzugriff (direkt oder ssh) auf die MSE.
- **WCS:** Standardmäßig verwendet WCS HTTPS, um mit MSE zu kommunizieren. HTTP kann über die WCS-GUI aktiviert werden.

In einigen Fällen kann WCS nicht über HTTPS mit MSE kommunizieren. In diesem Fall meldet das Hinzufügen von MSE zu WCS oder die Seite "Save on MSE General Properties" (Allgemeine

Eigenschaften für MSE speichern) den Fehler "HTTPS-Verbindung zum Server fehlgeschlagen". MSE muss von WCS aus pingbar (erreichbar) sein, und der Befehl "getserverInfo" auf MSE stellt Statusinformationen bereit. Es wird empfohlen, HTTP auf MSE zu aktivieren und WCS über HTTP mit MSE zu kommunizieren.

Auf MSE ist HTTP-Unterstützung in den Versionen 5.1, 5.2 und 6.0 verfügbar.

Aktivieren Sie HTTP auf MSE, die Version 6.0 der Softwareversion ausführt: Melden Sie sich über ssh/console bei der MSE an. Geben Sie den folgenden Befehl ein:

```
root@mse ~]# enablehttp
```

Aktivieren Sie HTTP auf MSE, die Version 5.x der Softwareversion ausführt: Melden Sie sich über ssh/console bei der MSE an. Geben Sie den folgenden Befehl ein:

```
[root@mse ~]# getdatabaseparams  
<DB PASSWORD>
```

Dieser Befehl gibt das db-Kennwort zurück. Verwenden Sie dieses Kennwort in diesem Befehl:

```
[root@mse ~]# /opt/mse/locserver/bin/tools/solid/solsql "tcp 2315" dba <DB PASSWORD>  
Solid SQL Editor (teletype) v.06.00.1049  
Copyright ©) Solid Information Technology Ltd 1993-2008  
Connected to 'tcp 2315'.  
Execute SQL statements terminated by a semicolon.  
Exit by giving command: exit;
```

```
update AESSERVERINFO set USEHTTP=1;  
Command completed successfully, 1 rows affected.
```

```
commit work;  
Command completed successfully, 0 rows affected.
```

Drücken Sie Control-C, um die Datenbank-Shell zu verlassen. MSE-Plattform-Neustart mit
/etc/init.d/msed stop /etc/init.d/msed start.

HTTP-Kommunikation von WCS (führt Software 6.x aus) zu MSE aktivieren:

- Stellen Sie sicher, dass HTTP auf MSE mit den vorherigen Schritten aktiviert ist.
- Wählen Sie in WCS auf der Seite Allgemeine Eigenschaften von MSE die Option HTTP aus. Dadurch wird die HTTP-Kommunikation zwischen WCS und MSE ermöglicht. Siehe **Abbildung 47**.

WCS kommuniziert nun über HTTP mit MSE.

Hinweis: Informationen zum Aktivieren von HTTP auf WCS 5.2 finden Sie im [WCS 5.2-Konfigurationshandbuch](#).

Abbildung 47: Aktivieren der HTTP-Kommunikation zwischen MSE und WCS

System

- General Properties
- NMSP Parameters
- Active Sessions
- Trap Destinations
- Advanced Parameters
- Logs
- Accounts
- Status
- Maintenance
- Context Aware Service
- wIPS Service

General Properties: MSE4

Services > Mobility Services > System > General Properties

General
Performance

Server Details

Device Name	MSE4
Device Type	Cisco 3350 Mobility Services Engine
Device UDI	"AIR-MSE-3350-K9:V01:MXQ828A4L9"
Version	6.0.62.0
Start Time	5/6/09 5:43 PM
IP Address	172.20.224.30
Contact Name	<input type="text" value="Joe"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
HTTP	<input checked="" type="checkbox"/> Enable
Legacy Port	<input type="text" value="8001"/>
Legacy HTTPS	<input type="checkbox"/> Enable

MSE-Lizenzierung

MSE-Lizenzen sind erforderlich, um kontextbezogene Informationen über Tags und Clients von Access Points ab 6.0-Code abzurufen. Die Lizenz des Clients umfasst die Verfolgung von Wireless-/kabelgebundenen Clients, nicht autorisierten Clients und nicht autorisierten Access Points. Lizenzen für Tags und Clients werden separat angeboten. Lizenzen für Tags und Clients werden in einer Reihe von Mengen angeboten, die zwischen 1.000, 3.000, 6.000 und 12.000 Geräte liegen. Cisco bietet Lizenzen für Clients und Tags an. Die Erstellung von Lizenzen und die Verwaltung von SKU-bezogenen Informationen erfolgt über das FlexLM-Lizenzsystem, das vom SWIFT-Team entwickelt und verwaltet wird.

WCS ist das Managementsystem für die Installation von Client- und wIPS-Lizenzen auf MSE. Lizenzen für Tags müssen über AeroScout aktiviert und mit dem AeroScout Systems Manager auf der MSE installiert werden.

Ausführliche Informationen zur MSE-Lizenzierung finden Sie in der [Lizenzierungs- und Bestellanleitung für die Cisco Mobility Services Engine der Serie 3300](#).

Neue Einkäufe

Kunden

- Der Kunde erwirbt eine SW-Lizenz und erhält den Product Authorization Key (PAK) per Post (Lizenzdokument).
- Der Kunde registriert PAK für Clients auf <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (nur registrierte Kunden).
- Geben Sie im Feld "Host-ID" die MSE UDI-Informationen ein. Akzeptieren Sie die Vereinbarung, und fahren Sie fort. Die Lizenz wird dem Kunden per E-Mail zugesandt.

- MSE UDI kann im WCS über die folgenden Registerkarten abgerufen werden: **Dienste > Mobilitätsdienste > MSE > System > Allgemeine Eigenschaften**
- Ohne Lizenz bietet die MSE 60 Tage lang die Funktion "Try before you Buy" (Testlizenz).
- Die Testlizenz ist nutzungsbasiert und 60 Tage lang gültig. Sie kann nur einmal verlängert werden.
- Lizenzbeschränkungen für die Evaluation: Clients: 100 Tags: 100 wIPS-APs: 20
- Evaluierungslizenzen werden immer erzwungen. Wenn jedoch die Plattformgrenze basierend auf den installierten Lizenzen erreicht wurde, kann die Evaluierungslizenz für einen separaten Service weiterhin verwendet werden. Wenn ein Kunde beispielsweise über eine MSE-3350 verfügt und Lizenzen für die Nachverfolgung von 18.000 Geräten (Clients und/oder Tags) installiert hat und 18.000 Geräte aktiv überwacht werden, kann er dennoch eine Evaluierungslizenz für wIPS verwenden, auch wenn die Plattformgrenze überschritten wird.
- Der Testlizenz-Timer beginnt ab dem Tag, an dem er generiert wird. Daher muss die Erweiterung der Testlizenz sofort installiert werden.
- Sobald die Lizenz installiert ist, ist sie abhängig von der Nutzung des Dienstes aktiviert/deaktiviert.
- Wenn die Testlizenz abläuft und die MSE nicht neu gestartet wird, werden die MSE-Kerndienste weiterhin ausgeführt, und lizenzierte Dienste wie Context Aware werden ebenfalls ausgeführt, Geräte werden jedoch nicht verfolgt.
- Wenn die Testlizenz abläuft und die MSE neu gestartet wird, werden die lizenzierten Dienste nicht gestartet. Geräte werden nicht verfolgt.

Wenn Sie keinen PAK haben

- Rufen Sie das Sales Order Status Tool unter <http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen> auf.
- Wählen Sie in der Dropdown-Liste Art der Abfrage die Option **Verkaufsauftrag aus**.
- Geben Sie die Verkaufsauftragsnummer im Feld Wert ein.
- Anzeigen mit **Aktivieren der Option Seriennummer anzeigen** und auf **Suchen** klicken.
- Das Fenster mit den Informationen zur MSE-Bestellung wird angezeigt.
- Klicken Sie in der Tabelle im Detailfenster "Bestellung" auf **Posten 1.1 erweitern**.
- Kopieren Sie in der Spalte "Produkt" (zweite Zeile) die PAK-Nummer (beginnt mit 3201J), die Sie registrieren möchten, um die Lizenz zu erhalten.
- Um PAK zu registrieren, besuchen Sie <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (nur registrierte Kunden).
- Klicken Sie links auf den Link zur Registrierung der Produktlizenz, geben Sie die PAK-Nummer in das leere Feld ein, und senden Sie sie.
- Geben Sie die MSE UDI-Informationen in das Feld Host-ID ein. Akzeptieren Sie die Vereinbarung, und fahren Sie fort.
- Es wird eine Lizenz generiert und eine E-Mail an Ihre E-Mail-ID gesendet.

Tags

1. Der Kunde erwirbt die Softwarelizenz und erhält den PAK (Product Authorization Key) per Post (Lizenzdokument).
2. Der Kunde registriert den PAK für Tags unter <http://support.AeroScout.com> .
3. Wenn Sie kein Konto haben, erstellen Sie ein neues Konto mit dem Link "Neues Konto erstellen".
4. Nachdem das Konto erstellt wurde, erhalten Sie eine Benachrichtigungs-E-Mail, die Ihren Benutzernamen und Ihr Kennwort enthält.

5. Melden Sie sich beim [AeroScout Support Portal](#) an.
6. Klicken Sie auf der Registerkarte "Startseite" auf den Link "Von Cisco gekaufte Produkte registrieren".
7. Registrieren Sie Ihre Produkte, und geben Sie die Kontaktdaten, PAK#, MSE ID (MSE S\N) und den Installationstyp an. Sie erhalten eine E-Mail-Nachricht, die die Registrierung bestätigt.
8. Die SE-Seriennummer kann von den Registerkarten "WCS" bezogen werden: **Services > Mobility-Services > MSE > Erweiterte Parameter**
9. AeroScout überprüft Ihre PAK-Nummer innerhalb von zwei Werktagen. Nach der Verifizierung erhalten Sie eine Benachrichtigung mit Ihrem Lizenzschlüssel, Anweisungen zum Herunterladen von Context Aware Engine SW sowie entsprechende Benutzerhandbücher an Ihre E-Mail-Adresse. Wenn Ihre PAK-Nummer ungültig ist, werden Sie aufgefordert, erneut eine gültige PAK-Nummer zu registrieren.

Upgrade - Client-Lizenz

1. Der Kunde erwirbt die neue Lizenz und erhält PAK per Post.
2. Der Kunde erhält den PAK und per E-Mail den Lizenzschlüssel.
3. Der Kunde installiert den Lizenzschlüssel auf der MSE.
4. **Hinzufügen der Anzahl der Evaluierungslizenzen (wenn die Anzahl der vorhandenen/installierten Clientlizenzen MSE max. entspricht):** WCS ermöglicht das Hinzufügen der Evaluierungslizenz, obwohl die maximale Anzahl an Geräten (Clients) für MSE erreicht wurde. Wenn der Kunde beispielsweise über MSE-3350 verfügt, über eine 18.000-Client-Lizenz verfügt und Tag-Tracking und/oder wIPS hinzufügen möchte, kann WCS eine Evaluierungslizenz für einen oder beide Dienste hinzufügen.

Upgrade - Tag-Lizenz

- **Hinzufügen der Tag-Lizenzanzahl (wenn die Anzahl der vorhandenen/installierten Tag-Lizenzen unter der maximal zulässigen MSE liegt):** Die vorhandene Tag-Lizenz wird durch eine neue Lizenz überschrieben. Wenn ein Kunde beispielsweise über eine vorhandene Lizenz zum Nachverfolgen von 1K-Tags verfügt und ein Upgrade auf die Nachverfolgung von 4K-Tags durchführen möchte, erwerben er eine 3K-Lizenz, um die vorhandene 1K-Lizenz zu erweitern. AeroScout stellt eine 4.000-Tag-Lizenz für die gesamte neue Tag-Anzahl aus.
- **Hinzufügen der Tag-Lizenzanzahl (wenn die Anzahl vorhandener/installierter Tag-Lizenzen MSE max. entspricht):** Der AeroScout System Manager gibt eine Fehlermeldung zurück. Die vorhandene Tag-Lizenz bleibt erhalten. Der Kunde hat beispielsweise MSE-3350 und eine 18 K-Tag-Lizenz auf der MSE installiert. Wenn Sie versuchen, eine 3K-Tag-Lizenz zu installieren, gibt AeroScout System Manager eine Fehlermeldung aus. Die Tag-Lizenz muss manuell aus MSE gelöscht werden, da der AeroScout System Manager keine Taglizenzen löschen kann. Um die neue Tag-Lizenz zu löschen, muss der Kunde das MSE-Image deinstallieren, die Datenbankoption entfernen und die MSE-Software neu installieren.
- **Hinzufügen der Anzahl der Evaluierungslizenzen (wenn die Anzahl der vorhandenen/installierten Tag-Lizenzen der MSE-Höchstzahl entspricht):** WCS ermöglicht das Hinzufügen einer Evaluierungslizenz, obwohl die maximale Anzahl an Geräten (Tag) für MSE erreicht ist. Wenn der Kunde beispielsweise über MSE-3350 verfügt, eine 18-K-Tag-Lizenz installiert hat und Client-Tracking und/oder wIPS hinzufügen möchte, kann er eine Evaluierungslizenz für einen oder beide Dienste hinzufügen.

Bestehende Kunden (gilt nur beim Upgrade auf 6.0-Softwareversion)

1. Besuchen Sie <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (nur registrierte Kunden), um den PAK für Kunden zu registrieren und den Lizenzschlüssel zu erhalten, wie oben im Abschnitt "Neue Einkäufe" beschrieben. Wenn der PAK ausgetauscht wurde, muss der Kunde das Cisco TAC/GLO anrufen.
2. Installieren Sie die Lizenzdatei auf MSE über WCS.
3. Die Lizenz ist an die MSE UID gebunden.
4. Besteht aus einer Plattform (MSE 3310 oder 3350) und einer eindeutigen Seriennummer. UDI-Beispiel: AIR-MSE-3310-K9:V01:QCN1224001Y. In diesem Beispiel ist die Seriennummer QCN1224001Y.
5. Die MSE-Lizenz ist an den Unique Device Identifier (UDI) gebunden. Wenn dieselbe Einheit reparierbar ist, ist die UDI dieselbe, und die gleiche Lizenz kann neu gehostet werden. Wenn die Einheit jedoch ersetzt werden muss, ändert sich die UDI, sodass eine neue Lizenz generiert werden muss. Die MSE akzeptiert die Lizenz nicht, wenn die UDI nicht übereinstimmt. Kunden können das Cisco TAC anrufen und die alte und neue UDI bereitstellen. Cisco TAC deaktiviert die alte Lizenz und gibt eine neue heraus.
6. Die MSE-3350 kann bis zu 18.000 Geräte (eine beliebige Kombination von Clients und Tags) mit dem richtigen Lizenzkauf verfolgen. Über den Cisco Wireless LAN Controller erhält die Mobility Services Engine Updates zu den Standorten der verfolgten Elemente.
7. In Cisco WCS-Maps, -Abfragen und -Berichten können nur die Elemente angezeigt werden, die für die Verfolgung durch den Controller vorgesehen sind. Für nicht nachverfolgte Elemente werden keine Ereignisse oder Alarmer gesammelt, und es werden keine Ereignisse verwendet, um den Grenzwert von 18.000 Elementen für Clients oder Tags zu berechnen.

Nach der erfolgreichen Installation der Lizenz wird der Lizenztyp jetzt als "Permanent" (dauerhaft) angezeigt, wie in **Abbildung 48** dargestellt.

Abbildung 48: Lizenzcenter

License Center

Administration > License Center > Summary > MSE Summary

Entries 1 - 3 of 3							
MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
(H) mse-3350 (AIR-MSE-3350-K9:V01:MXQ821A31P)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (60 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (60 days left)	Active
(H) heitz-3350 (AIR-MSE-3350-K9:V01:USE810N5HR)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (59 days left)	Active
	Tag Elements	100	5	0	5%	Evaluation (59 days left)	Active
	Client Elements	100	100	372	100%	Evaluation (59 days left)	Active
(L) heitz-3310 (AIR-MSE-3310-K9:V01:QSH78150059)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (Less than a day left)	Inactive
	Tag Elements	1000	4	0	0%	Permanent	Active
	Client Elements	1000	667	0	66%	Permanent	Active

Hinweis: Wenn ein Client oder Tag 24 Stunden lang inaktiv ist, werden sie nicht mehr auf die entsprechende Lizenzanzahl angerechnet.

Die Lizenzdatei wird unter "opt/mse/licensing" gespeichert.

Wenn Sie ein Upgrade von MSE 5.x auf 6.x durchführen, stellen Sie sicher, dass die folgenden Schritte nacheinander ausgeführt werden:

1. Führen Sie mit WCS eine MSE-Datenbanksicherung für MSE 5.x durch, das heißt das derzeit ausgeführte MSE-System.
2. Informationen zum Sichern von Daten und der Konfiguration für Tags finden Sie im [Konfigurationsleitfaden für kontextsensitive Service-Software](#).
3. Aktualisieren Sie MSE auf die Software 6.x. Die Warnmeldungen werden im Aktualisierungsprozess der MSE über "Lizenzierung" bei der Installation angezeigt.
4. Installieren Sie die MSE-Lizenz über WCS. Eine Warnmeldung zeigt an, ob eine Lizenz, die die MSE-Systemkapazität überschreitet, installiert und der Lizenzinstallationsprozess blockiert wird. Wenn ein Kunde beispielsweise über eine MSE-3310 verfügt und versucht, eine 6K-Client-Lizenz zu installieren, wird eine Warnmeldung angezeigt, da eine MSE-3310 maximal 2.000 Geräte überwachen kann.
5. Stellen Sie die MSE-Datenbank mit WCS wieder her.
6. Um Daten und Konfigurationen für die Tag-Engine wiederherzustellen, folgen Sie der [AeroScout-Dokumentation](#).
7. Einzelheiten zu diesen Schritten finden Sie in Anhang B dieses Dokuments und im [kontextsensitiven Konfigurationsleitfaden für Version 6.x](#). **Hinweis:** Mit der Softwareversion 6.0 für die Tag-Nachverfolgung bleiben die AeroScout-Engine-Konfigurationen und Lizenzdaten in WCS/MSE-Sicherungs- und Wiederherstellungsprozessen erhalten. Jede auf MSE ausgeführte Konfiguration, die eine Softwareversion vor 6.0 ausführt, wird nicht automatisch beibehalten. Bei einem Upgrade von 6.0 auf 6.x werden diese Konfigurationsdaten beibehalten, wenn Sie das MSE-Sicherungs-/Wiederherstellungsverfahren verwenden, wie in der Cisco Dokumentation beschrieben. Wenn ein Kunde ein Upgrade von 5.2 auf 6.0 durchführt, muss er das manuelle Verfahren gemäß der [AeroScout-Dokumentation](#) befolgen. **Achtung:** Die Anzahl der unterstützten Clients, Tags und Access Points (wlPS) wird auf 100 Clients, 100 Tags und 20 APs zurückgesetzt, wenn Sie ein Upgrade auf Version 6.x durchführen, wenn keine entsprechende Lizenz vorhanden ist. Alle bis auf 100 Elemente sind als inaktiv gekennzeichnet. Die Verlaufsdaten für alle verfolgten Elemente verbleiben in der Datenbank und können innerhalb der Standort-API der MSE abgefragt werden. Diese Beschränkungen entsprechen Evaluierungslizenzen für 60 Tage, die standardmäßig für nicht lizenzierte MSE bereitgestellt werden.

Ändern Sie diese Verfolgungsparameter mit Cisco WCS (siehe **Abbildung 49**):

1. Aktivieren und Deaktivieren von Elementstandorten (kabelgebundene/Wireless-Clients, aktive Ressourcen-Tags sowie nicht autorisierte Clients und Access Points), die Sie aktiv überwachen.
2. Legen Sie Grenzwerte für die Anzahl der Elemente fest, die überwacht werden sollen.
3. Wenn Sie beispielsweise eine Client-Lizenz von 12.000 nachverfolgbaren Geräten (kabelgebunden/drahtlos) besitzen, können Sie ein Limit festlegen, um nur 8.000 Client-Stationen zu überwachen (wodurch 4.000 Geräte für die Nachverfolgung von nicht autorisierten Clients und nicht autorisierten Access Points verfügbar bleiben). Sobald der Verfolgungsgrenzwert für ein bestimmtes Element erreicht ist, wird die Anzahl der nicht nachverfolgten Elemente auf der Seite Verfolgungsparameter zusammengefasst.
4. Die Nachverfolgung und Berichterstellung von nicht autorisierten Ad-hoc-Clients und Access Points wird deaktiviert.

Abbildung 49: Verfolgungsparameter für kontextsensitive Dienste

Tracking Parameters: MSE4
 Services > Mobility Services > Context Aware Service > Administration > Tracking Parameters

The SNMP parameters and Polling Interval are applicable for Controller version 4.1 or below

Tracking Parameters

Network Location Service Elements:		Licensed Limit = 6000			
Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Wireless Clients	<input checked="" type="checkbox"/>	200	323	0
<input checked="" type="checkbox"/>	Wired Clients	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Rogue Clients and AccessPoints	<input type="checkbox"/>	0	1149	0
<input type="checkbox"/> Exclude Adhoc Rogue APs					

Asset Tracking Elements:		Licensed Limit = 100			
Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Active RFID Tags	<input type="checkbox"/>	100	20	0

Die tatsächliche Anzahl der verfolgten Clients hängt von der erworbenen Lizenz ab.

Aktiver Wert (siehe Abbildung 49): Zeigt die Anzahl der Clientstationen an, die derzeit überwacht werden.

Nicht verfolgt (siehe Abbildung 49): Gibt die Anzahl der Client-Stationen an, die über den Grenzwert hinausgehen.

Überschüssige Elemente (Tags/Clients/Schurken) werden nicht nachverfolgt, wie in Abbildung 50 gezeigt.

Abbildung 50: Lizenznutzung

MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
mse-3350 (AIR-MSE-3350-K9:V01:MXQ821A31P)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (60 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (60 days left)	Active
heitz-3350 (AIR-MSE-3350-K9:V01:USE810N5HR)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (59 days left)	Active
	Tag Elements	100	5	0	5%	Evaluation (59 days left)	Active
	Client Elements	100	100	372	100%	Evaluation (59 days left)	Active

Wie mehrere Services skaliert werden

Die MSE mit der 6.0-sw-Version unterstützt den gleichzeitigen Betrieb von kontextsensitivem und WIPS. Es werden Beschränkungen für die Koexistenz von Funktionen durchgesetzt. Über die Limitkombinationen hinaus werden keine TAC unterstützt und sind nicht einmal möglich, da keine Lizenz hinzugefügt werden kann, die zu einer Überschreitung der MSE-Kapazität führt.

Die unterstützten Kombinationen sind in den Abbildungen 51 und 52 dargestellt.

Abbildung 51: MSE-3350-Systemkapazität: APs und kontextsensitive Geräte im wIPS-Überwachungsmodus

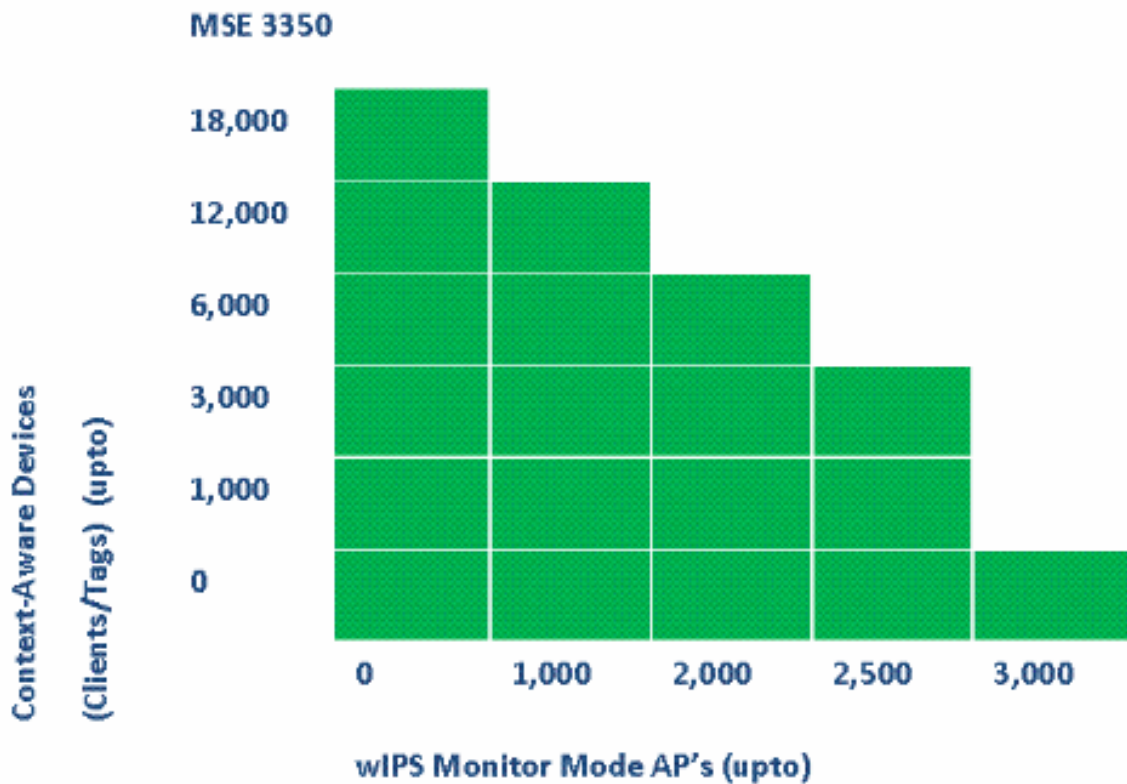
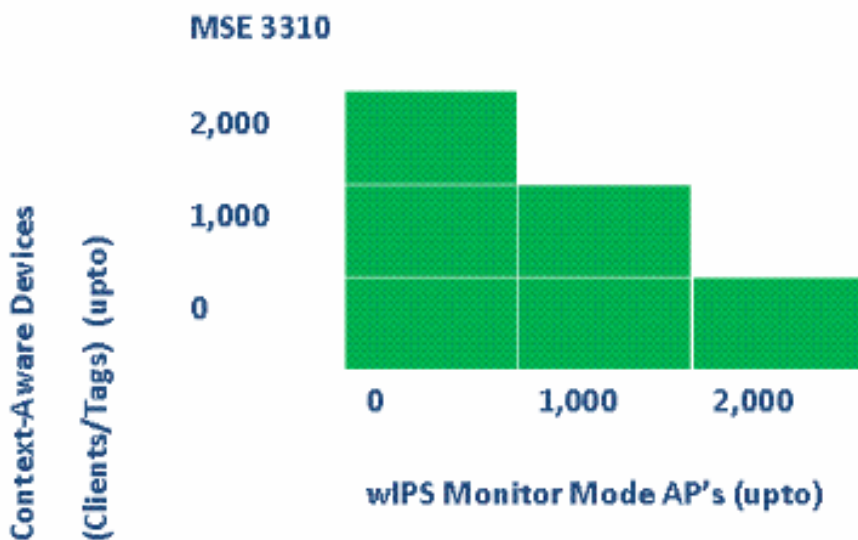


Abbildung 52: MSE-3310-Systemkapazität: APs und kontextsensitive Geräte im wIPS-Überwachungsmodus



Einige Beispiele:

- Der Kunde möchte 6.000 Geräte mithilfe des kontextsensitiven Services nachverfolgen.

Anschließend kann er bis zu 2.000 wIPS-Überwachungsmodus-APs auf der MSE 3350 nutzen.

- Der Kunde möchte 3K-Geräte mithilfe des kontextsensitiven Services nachverfolgen, kann dann bis zu 2.500 wIPS Monitor Mode-APs auf der MSE 3350 nutzen.
- Der Kunde möchte 1K-Geräte mithilfe des kontextsensitiven Services nachverfolgen. Anschließend kann er bis zu 1.000 wIPS Monitor Mode-APs auf der MSE 3310 und 2.500 wIPS Monitor Mode-APs auf der MSE 3350 überwachen.

Fehlerbehebung

MSE ist nicht erreichbar

Wenn MSE aus WCS-Sicht als nicht erreichbar erkannt wird, können folgende Gründe vorliegen:

- Die Anmeldeinformationen für die API im WCS werden falsch konfiguriert. Die Appliance verfügt über zwei Berechtigungssätze: Eine ist für die Appliance-Shell-Schnittstelle und eine andere für die API-Anmeldeinformationen. WCS benötigt die API-Anmeldeinformationen, wenn MSE hinzugefügt wird. Siehe Anhang A dieses Dokuments.
- Regeln für Routen- und Firewall-Verbindungen blockieren die Verbindung zwischen WCS und MSE. Weitere Informationen finden Sie im Abschnitt "Überprüfen der Netzwerkverbindung" in diesem Dokument.
- Die WCS-Hintergrundaufgabe "Mobility Service Status" wurde deaktiviert. Aktivieren Sie es in WCS durch **Administration > Background Tasks > Other Background Tasks > Mobility Service Status (Verwaltung > Hintergrundaufgaben > Andere Hintergrundaufgaben > Mobilitätsdienststatus)**.
- Die MSE Service Context Aware (MSE-Servicekontextsensitivität) ist über die MSE-CLI aktiviert und aktiviert.
- In seltenen Fällen kann HTTPS ein Verbindungsproblem haben. Sie können die HTTP-Option unter MSE General Properties in WCS aktivieren. Weitere Informationen finden Sie im Abschnitt "WCS/MSE Communication" dieses Dokuments.
- MSE ist abgestürzt. Bei MSE kann CLI "getserverInfo" keine Ausgabe zurückgeben. Sammeln Sie alle Protokolle im Verzeichnis "under/opt/mse/logs", und wenden Sie sich an das Cisco TAC.

Keine Elemente gefunden

Wenn sich in der MSE keine Elemente befinden, können folgende Gründe vorliegen:

- MSE ist nicht erreichbar.
- Die Testlizenz ist abgelaufen.
- MSE ist erreichbar, und es wird eine Lizenz angewendet, aber der MSE Context Aware Module Service ist nicht aktiviert.
- Die Nachverfolgung für Clients und/oder Tags ist auf der Seite MSE Tracking Parameters (MSE-Nachverfolgungsparameter) nicht aktiviert. Weitere Informationen finden Sie im Abschnitt "MSE-Lizenzierung" dieses Dokuments.
- Netzwerkdesigns und/oder Controller wurden nicht mit der MSE synchronisiert.
- Access Points wurden nicht auf WCS-Karten positioniert.
- Zwischen MSE und Controller sind keine NMSP-Verbindungen eingerichtet. Weitere Informationen finden Sie im Abschnitt "Überprüfen der NMSP-Verbindung zwischen WLC und

MSE" dieses Dokuments.

- Access Points im WCS verfügen über Antennen von Drittanbietern (Typ gewählt wurde "Other"). In diesem Fall müssen die Access Points im WCS auf einen anderen, ähnlich unterstützten Antennentyp eingestellt und das Netzwerkdesign mit MSE re-synchronisiert werden.
- Der Wireless LAN Controller (WLC) erkennt keine Clients. Fehlerbehebung für WLC mit CLI "show client summary".
- Der Wireless LAN Controller (WLC) erkennt keine aktiven RFID-Tags. Fehlerbehebung für WLC mit CLI "show rfid summary".

Tags sind nicht vorhanden

Wenn Tags nicht gefunden werden (aber andere Clients sind), kann ein Problem innerhalb der AeroScout-Engine auftreten. Mögliche Gründe sind:

- Aktive RFID-Tags werden vom WLC nicht verfolgt. Dieser Befehl muss in der WLC-Konfiguration vorhanden sein: `config rfid status enable`.
- Der Wireless LAN Controller (WLC) erkennt keine aktiven RFID-Tags. Fehlerbehebung für WLC mit CLI "show rfid summary".
- Tags werden von WLC erkannt, jedoch nicht in WCS. Überprüfen Sie, ob die NMSP-Benachrichtigung mit dem folgenden Befehl an die MSE gesendet wird: `debug rfid nmstp enable`.
- Die AeroScout-Engine ist nicht in MSE installiert. In den Versionen 5.1 und 5.2 muss der Motor separat installiert werden. Ab Version 6.0 ist die Engine mit MSE gebündelt.
- Die Lizenz ist für die AeroScout Engine nicht installiert.
- Die AeroScout-Engine lässt sich nicht bei MSE registrieren. Überprüfen Sie die Partner Engine-Statusseite in WCS.
- MSE enthält zu viele Karten, oder die Karten sind zu groß. Weitere Informationen finden Sie in den Richtlinien der AeroScout-Engine.
- Nach einem Upgrade muss die Konfiguration möglicherweise wieder auf der AeroScout-Engine ausgeführt werden.
- Die Bodenkarte hat kein Bild (wurde in den letzten Versionen aufgelöst).
- MSE verfolgt nur CCX-kompatible Tags, und die Bereitstellung hat nur nicht unterstützte, nicht CCX-konforme Tags oder wurde nicht für die Übertragung im CCX-Format konfiguriert.

Bestimmte Elemente sind nicht vorhanden (Clients oder Tags)

Wenn die MSE bestimmte Elemente verfolgt, andere jedoch nicht sichtbar sind, können folgende Gründe vorliegen:

- MSE wird auf einer Evaluierungslizenz ausgeführt, die auf 100 Elemente beschränkt ist.
- MSE läuft mit einer gültigen Lizenz, aber die Kapazität wurde überschritten, sodass alle zusätzlichen Elemente (Clients/Tags/Rogues) verworfen werden.
- Bestimmte Controller verfügen nicht über NMSP-Verbindungen mit MSE.
- Das Element ist aus dem Netzwerk verschwunden und überträgt nicht mehr. MSE speichert das Element in seinem Verlaufsprotokoll, verschwindet jedoch von WCS-Bildschirmen.
- Filteroptionen wurden in WCS-Karten-Layern angewendet, sodass einige Elemente angezeigt werden konnten.
- MAC-Filterungsoptionen sind in MSE-Filterungsparametern aktiviert, wobei einige Elemente verworfen werden.

- MSE verfolgt nur CCX-kompatible Tags. Die Bereitstellung verfügt über eine Kombination aus CCX- und Nicht-CCX-Tags.
- Erweiterung zur Client/Tag-Fehlerbehebung für den Standort:Überprüfen Sie, ob WCS diesen Client sieht oder nicht. Über SNMP existiert diese Funktionalität bereits für Clients. (Client-Fehlerbehebung). Dies muss für Tags erweitert werden.Suchen Sie nach dem Client am zugewiesenen Standort. Verwenden Sie den WLC-Befehl **show client summary**.Stellen Sie fest, wie lange der Client vor WLC die WLC-Befehle **show client <MAC-Adresse> detail** verwendet.Stellen Sie fest, wann APs den Client zum letzten Mal mithilfe des WLC-Befehls **anzeigen, dass der Client <MAC-Adresse> Details enthält**.

WLC nicht mit MSE verbunden

Wenn ein Controller keine Verbindung mit der MSE herstellt, können folgende Ursachen auftreten:

- Controller ist aus MSE- oder WCS-Perspektive nicht erreichbar.
- Das WCS hatte ein temporäres Verbindungsproblem mit dem Controller und konnte den Hash-Sicherheitsschlüssel für die NSMP-Verbindung nicht übertragen. Überprüfen der SNMP-Verbindung zwischen WCS und Controller
- Der Controller und die MSE verfügen nicht über eine richtige NTP-Konfiguration, oder der Zeitunterschied zwischen diesen Konfigurationen ist erheblich. Konfigurieren Sie die Zeiten korrekt.
- Controller, die älter als Version 4.2 sind, unterstützen NMSP nicht.
- Controller, die vor Version 5.1 veröffentlicht wurden, unterstützen nicht mehrere MSE-Verbindungen.
- Wenn ein Controller einer MSE mit aktiviertem wIPS zugewiesen wird, kann derselbe Controller nicht gleichzeitig einer anderen MSE zugewiesen werden.
- WCS verfügt nach der Synchronisierung nicht über Lese-/Schreibzugriff auf den WLC. Dies führt dazu, dass das WCS die MSE-MAC und den Schlüssel-Hash nicht an den WLC übertragen kann.

Benachrichtigungen erreichen keine externen Partneranwendungen

In Fällen, in denen eine Partneranwendung keine Benachrichtigungen von der MSE erhält, kann dies folgende Gründe haben:

- Die Verbindung zwischen der MSE und der externen Anwendung ist nicht hergestellt. Überprüfen des XML/API-Datenverkehrs
- Die Anwendung des externen Listeners ist ausgefallen.
- Der externe Listener analysiert langsam die eingehenden Benachrichtigungen. In diesem Fall wartet die MSE auf die Verarbeitung eines externen Listeners, was zu einer Überlastung der ausgehenden MSE-Warteschlangen führen kann.
- Die MSE verwirft Benachrichtigungen aufgrund der relativ geringen Größe ihrer ausgehenden Warteschlange im Vergleich zur erwarteten Anzahl von Tag-Benachrichtigungs-Frames im Netzwerk. Überprüfen Sie, ob die Tags eine angemessene Konfiguration aufweisen, insbesondere für die Beschleunigung/Entbeschleunigung von Bewegungen. Erhöhen Sie die Warteschlangengröße in den MSE Notification Parameters. Weitere Informationen finden Sie im Abschnitt "Northbound Notification" in diesem Dokument.

Kabelgebundener Standort funktioniert nicht

Wenn beim Verwenden des kabelgebundenen Standorts keine Elemente nachverfolgt werden,

können folgende Gründe vorliegen:

- NMSP-Verbindungsprobleme zwischen MSE und kabelgebundenen Switches.
- Der kabelgebundene Switch führt eine ältere Version aus, die den kabelgebundenen Standort nicht unterstützt.
- Der kabelgebundene Switch hat die richtige Version, aber NMSP ist nicht aktiviert. Aktivieren Sie es mit der CLI-Option.
- Der kabelgebundene Switch muss über eine IP-Nachverfolgungsoption verfügen, um die Nachverfolgung der angeschlossenen Clients zu starten.
- Der kabelgebundene Switch wurde dem WCS nicht hinzugefügt.
- Mögliche Probleme beim Hinzufügen eines kabelgebundenen Switches in WCS:Falsche SNMP-Community-Strings.Switch-OID wird in WCS nicht unterstützt.
- Der kabelgebundene Switch wurde dem WCS hinzugefügt, ist aber nicht mit der MSE synchronisiert.
- Der kabelgebundene Switch ist für die Synchronisierung verfügbar. Überprüfen Sie, ob der Switch mit dem in WCS aktivierten Flag "Location Capable" (Standort-fähig) hinzugefügt wurde.
- Die kabelgebundenen Switches unterstützen nur eine NMSP-Verbindung mit einer MSE.
- Die kabelgebundene Verfolgung ist in den MSE-Verfolgungsparametern nicht aktiviert.

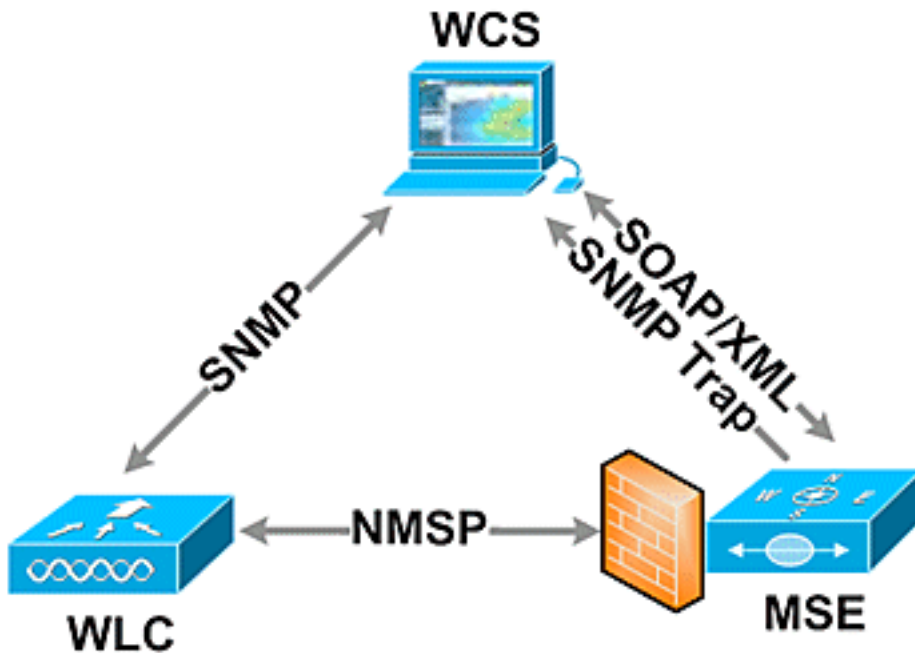
MSE-Lizenzierung

- Bei Installation der Lizenz wird eine Unstimmigkeitsmeldung für UDI angezeigt. MSE-Lizenzen sind an MSE UDI gebunden. Stellen Sie daher sicher, dass die installierte Lizenz für die richtige MSE erstellt wurde. Sie können Lizenzen nicht zwischen verschiedenen MSEs austauschen.
- Die Lizenzinstallation wird blockiert, da das Element die zulässige Grenze für diese MSE überschreitet. Überprüfen Sie die Lizenzkapazität für jeden Service auf verschiedenen MSE-Plattformen, wie im Abschnitt "Vorschau" beschrieben.
- Fehler können angezeigt werden, wenn Sie versuchen, zwei Lizenzen nacheinander zu installieren oder zu löschen. Der Grund hierfür ist, dass bei jeder Installation von CAS-Lizenzen der gesamte Dienstneustart sowie jedes Mal, wenn die wIPS-Lizenz installiert wird, der wIPS-Dienst neu gestartet wird. Bevor Sie sofort mit der Installation einer weiteren Lizenz fortfahren, stellen Sie sicher, dass alle Dienste verfügbar sind.
- MSE-Lizenzen werden unter /opt/mse/licenses installiert.

Überprüfung der Netzwerkverbindung

Stellen Sie sicher, dass keine Firewalls die Verbindung zwischen MSE, WLC und WCS blockieren. Wenn Sie eine Firewall von diesen Feldern installieren müssen, erstellen Sie Regeln für Platzhalter, damit diese Computer erfolgreich miteinander kommunizieren können (siehe **Abbildung 53**).

Abbildung 53: Überprüfung der Netzwerkverbindung



Überprüfen der NMSP-Verbindung zwischen WLC und MSE

```
(Cisco Controller) >show nmsp status
```

LocServer IP	TxEchoResp	RxEchoReq	TxData	RxData
172.20.224.17	18006	18006	163023	10

```
(Cisco Controller) >show auth-list
```

```
<snip>
```

Mac Addr	Cert Type	Key Hash
00:1e:0b:61:35:60	LBS-SSC	5384ed3cedc68eb9c05d36d98b62b06700c707d9

Wenn die NMSP-Verbindung nach dem Hinzufügen von MSE zum WCS nicht hergestellt wird, besteht ein möglicher Grund in der Uhrendiskrepanz zwischen WLC und MSE. Es wird empfohlen, zur Synchronisierung der Uhren einen NTP-Server zu verwenden. Ist dies nicht möglich, können die Uhren auf dem WLC und der MSE manuell konfiguriert werden. Das Hauptproblem bei den Systemuhren besteht darin, sicherzustellen, dass die WLC-Zeit nicht hinter der auf der MSE festgelegten Zeit zurückbleibt.

Hinweis: Die Zeitsynchronisierung zwischen den Controllern ist in großen, mehreren WLC-Bereitstellungen unerlässlich.

Wenn noch keine NMSP-Sitzung eingerichtet wurde, kann der Netzwerkadministrator eine NMSP-Sitzung manuell einrichten, indem er den MSE-Schlüssel-Hash in den WLC eingibt.

```
MSE
root@mse ~]# cmdshell
cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
-----
Server Auth Info
-----
MAC Address: 00:1e:0b:61:35:60
```

Key Hash: 5384ed3cedc68eb9c05d36d98b62b06700c707d9
Certificate Type: SSC

WLC
(Cisco controller) >config auth-list add lbs-ssc <MSE Ethernet MAC> <MSE key hash>

Überprüfung der Betriebsfähigkeit der MSE und Erhalt von Tag- und Client-Informationen vom WLC

Der Befehl **getserverinfo** auf der MSE liefert folgende Ausgabe:

```
[root@MSEWCS4 ~]# getserverinfo
MSE Platform is up, getting the status

-----
Server Config
-----

Product name: Cisco Mobility Service Engine
Version: 6.0.49.0
Hw Version: V01
Hw Product Identifier: AIR-MSE-3350-K9
Hw Serial Number: MXQ828A4L9
Use HTTP: false
Legacy HTTPS: false
Legacy Port: 8001
Log Modules: 262143
Log Level: INFO
Days to keep events: 2
Session timeout in mins: 30
DB backup in days: 2

-----
Services
-----

Service Name: Context Aware Service
Service Version: 6.0.35.0
Admin Status: Enabled
Operation Status: Up

Service Name: Wireless Intrusion Protection Service
Service Version: 1.0.1096.0
Admin Status: Enabled
Operation Status: Up

-----
Server Monitor
-----

Mon Mar 16 14:43:52 PDT 2009
Server current time: Thu Apr 02 14:55:00 PDT 2009
Server timezone: America/Los_Angeles
Server timezone offset: -28800000
Restarts: 3
Used Memory (bytes): 166925392
Allocated Memory (bytes): 238354432
Max Memory (bytes): 1908932608
DB virtual memory (kbytes): 6694
DB virtual memory limit (bytes): 0
DB disk memory (bytes): 241696768
```

DB free size (kbytes): 6304

Active Sessions

Session ID: 17155
Session User ID: 1
Session IP Address: 172.20.224.30
Session start time: Tue Mar 17 16:50:48 PDT 2009
Session last access time: Thu Apr 02 14:50:30 PDT 2009

Context Aware Service

Total Active Elements(Clients, Rogues, Interferers): 2263
Active Clients: 591
Active Tags: 24
Active Rogues: 1648
Active Interferers: 0
Active Wired Clients: 0
Active Elements(Clients, Rogues, Interferers) Limit: 6000
Active Tag Limit: 100
Active Wired Clients Limit: 0
Active Sessions: 1
Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogues Not Tracked due to the limiting: 0
Interferers Not Tracked due to the limiting: 0
Wired Clients Not Tracked due to the limiting: 0
Total Elements(Clients, Rogues, Interferers)
Not Tracked due to the limiting: 0

Context Aware Sub Services

Sub Service Name: AeroScout
Version: 3.2.0 - 4.0.14.9
Description: AeroScout@ Location Engine
for RSSI and TDOA asset tracking
Registered: true
Active: true
Watchdog Process ID: 8492
Engine Process ID: 8665
[root@MSEWCS4 ~]#

Überprüfen Sie, ob das RFID-Tag vom WLC erkannt wird.

Tags müssen für die Übertragung auf 3 Kanälen (1,6,11) und mit mindestens 3 Wiederholungen konfiguriert werden.

Beispiel: 1,6,11, 1,6,11, 1,6,11

Überprüfen Sie die globale RFID-Konfiguration auf dem Controller.

show rfid config

Wenn die RFID-Tag-Erkennung nicht aktiviert ist, aktivieren Sie sie mit dem folgenden Befehl:

```
config rfid status enable
```

Prüfen/Einstellen der Timeout-Parameter.

```
config rfid timeout 1200
```

```
config rfid auto-timeout disable
```

Überprüfen Sie das RSSI-Ablaufdatum.

```
show location summary
```

Wenn das Tag von WLC immer noch nicht erkannt wird, verwenden Sie die folgenden Debugbefehle:

```
debug mac addr <tag mac addr>
```

```
debug rfid receive enable
```

Überprüfen Sie, ob WLC das Tag erkennt.

```
show rfid summary
```

```
show rfid detail <MAC address>
```

Wenn das Tag vom WLC erkannt wird, aber nicht in WCS angezeigt wird, überprüfen Sie, ob NMSP-Benachrichtigungen an MSE gesendet werden.

```
debug rfid nmsp enable
```

Überprüfen Sie, ob die NMSP-Benachrichtigung auf dem WLC aktiviert ist.

```
show nmsp subscription summary
```

```
Server IPServices
```

```
<MSE IP>RSSI, Info, Statistics, IDS
```

Überprüfen Sie, ob die NMSP-Ebene auf dem WLC Benachrichtigungen sendet.

```
debug nmsp message tx enable
```

RSSI-Sperrung: Die MSE behält die vier höchsten Werte für die Signalstärke sowie alle Berichte zur Signalstärke bei, die den RSSI-Grenzwert erfüllen oder überschreiten. Standardwert = -75 dBm

show rfid summary-Befehl (WLC)

Dieser Befehl listet alle von APs gemeldeten RFID-Tags auf, die folgende Informationen enthalten:

- RFID-MAC-Adresse
- nächster AP
- RSSI-Wert
- Zeit seit dem letzten Anhören des Tags

```
(Cisco Controller) >show rfid summary
```

```
Total Number of RFID    : 4
```

RFID ID	VENDOR	Closest AP	RSSI	Time Since Last Heard
00:04:f1:00:04:ea	Wherenet	sjc14-42b-ap4	-69	52 seconds ago
00:04:f1:00:04:eb	Wherenet	sjc14-42b-ap4	-75	27 seconds ago
00:0c:cc:5b:fc:54	Aerosct	sjc14-31b-ap9	-87	63 seconds ago
00:0c:cc:5b:fe:29	Aerosct	sjc14-31b-ap2	-92	22 seconds ago

Befehl show rfid detail

Dieser Befehl enthält Parameterdetails für ein RFID-Tag, wenn er die MAC-Adresse angibt.

```
(Cisco Controller) >show rfid detail 00:0c:cc:5b:fe:29
```

```
RFID address..... 00:0c:cc:5b:fe:29
Vendor..... Aerosct
Last Heard..... 4 seconds ago
Packets Received..... 561211
Bytes Received..... 16836330
Detected Polling Interval..... 14 seconds
Bluesoft Type..... TYPE_NORMAL
Battery Status..... MEDIUM
Nearby AP Statistics:
    sjc14-41b-ap8(slot 0, chan 6) 3 seconds.... -88 dBm
```

```
(Cisco Controller) >
```

Überprüfen, ob der Wi-Fi-Client vom WLC erkannt wird

Bestimmen Sie, welchen APs der Client zugeordnet ist, und bestimmen Sie die von den APs erkannten RSSI-Werte.

```
show client summary
show client detail <MAC address>
```

Überprüfen Sie, ob die RSSI-Timeouts für den Client auf die Standardwerte eingestellt sind.

```
show location summary
```

Wenn sich die RSSI-Werte von den Standardwerten unterscheiden, legen Sie sie mit den folgenden Konfigurationsbefehlen auf die Standardwerte fest:

```
config location expiry client <seconds>
config location rssi-half-life client <seconds>
```

Aktivieren von Load-Balancing-Debuggen; zeigen, welche APs den Client gehört haben und mit welchem RSSI.

```
debug mac addr <client mac>
debug dot11 load-balancing enable
```

Debug-Benachrichtigungsprobleme mit diesen Befehlen:

```
debug mac addr <client mac>
debug dot11 locp enable
debug nmsp message tx enable
```

Befehl "show client summary"

(Cisco Controller) >show client summary

Number of Clients..... 276

<snip>

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth Protocol	Port	Wired
00:02:8a:ea:55:15	sjc14-12b-ap5	Associated	7	Yes 802.11b	2	No

Befehl "show client detail"

Cisco Controller) >show client detail 00:02:8a:ea:55:15

<snip>

Nearby AP Statistics:

TxExcessiveRetries: 0

TxRetries: 0

RtsSuccessCnt: 0

RtsFailCnt: 0

TxFiltered: 0

TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]

sjc14-11b-ap2(slot 0)

antenna0: 308 seconds ago -86 dBm.....

antenna1: 308 seconds ago -80 dBm

sjc14-11b-ap1(slot 0)

antenna0: 307 seconds ago -82 dBm.....

antenna1: 307 seconds ago -91 dBm

sjc14-12b-ap6(slot 0)

antenna0: 307 seconds ago -66 dBm.....

antenna1: 307 seconds ago -66 dBm

sjc14-12b-ap3(slot 0)

antenna0: 307 seconds ago -76 dBm.....

antenna1: 307 seconds ago -64 dBm

sjc14-12b-ap5(slot 0)

antenna0: 7217 seconds ago -53 dBm.....

antenna1: 7217 seconds ago -48 dBm

sjc14-11b-ap5(slot 0)

antenna0: 7217 seconds ago -79 dBm.....

antenna1: 7217 seconds ago -75 dBm

Abschnitt 4: Finale Checkliste

Hardware-Anforderungen

Tabelle 3: Cisco MSE 3310 - Hardwarespezifikationen

Element	Beschreibung
Formfaktor	1HE-Rack-Formfaktor 4,45 cm (1,75 Zoll) Höhe, 70,5 cm (27,75 Zoll) Tiefe
Prozessor	Intel Core2 Duo (1,8 GHz)
Arbeitsspeicher	4 GB (PC2-5300)
Festplatten	2 x 250 GB SATA
Kapazität	Bis zu 2.000 Geräte (bis zu 1.000 Clients)

für Standortverfolgung	und bis zu 1.000 Tags)
Konnektivität	Netzwerk: Zwei integrierte Multifunktions-Gigabit-Netzwerkadapter mit TCP/IP-Offload-Engine
Netzteile	Eine 120/240 V Wechselstrom
Netzwerkmanagement	Cisco WCS Location v5.2 oder höher mit Internet Explorer 6.0/Service Pack 1 oder höher
Unterstützte Netzwerkgeräte	Cisco Wireless LAN Controller der Serien 2100 und 4400 Cisco Catalyst Wireless Services Module der Serie 6500, Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM und WLCM-E) für Integrated Services Router Cisco Aironet Lightweight Access Points

Tabelle 4: Cisco MSE 3550 - Hardwarespezifikationen

Element	Beschreibung
Formfaktor	1HE-Rack-Formfaktor 4,45 cm (1,75 Zoll) Höhe, 70,5 cm (27,75 Zoll) Tiefe
Prozessor	Zwei Intel Xeon Quadcore-Prozessoren (2,33 GHz)
Arbeitsspeicher	8 GB PC2-5300 (4 x 2 GB)
Festplatten	Hot Plug SAS-Laufwerke (Serial Attached SCSI): 2 x 146 GB (10.000 U/Min)
Kapazität für Standortverfolgung	Bis zu 18.000 Geräte (beliebige Kombination aus Clients und Tags)
Konnektivität	Netzwerk: Zwei integrierte Multifunktions-Gigabit-Netzwerkadapter mit TCP/IP-Offload-Engine
Netzteile	Zwei redundante 120/240-V-Wechselstrom (Hot-Swap-fähig)
Netzwerkmanagement	Cisco WCS Location v5.1 oder höher mit Internet Explorer 6.0/Service Pack 1 oder höher
Unterstützte Netzwerkgeräte	Cisco Wireless LAN Controller der Serien 2100 und 4400 Cisco Catalyst Wireless Services Module der Serie 6500, Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM und WLCM-E) für Integrated Services Router Cisco Aironet Lightweight Access Points

Migration von Standortdiensten von Cisco 2710 auf Cisco MSE

Vor der Einführung der MSE-Plattform bot Cisco mit der auf der Cisco Serie 2710 basierenden Lösung standortbasierte Services an. **Tabelle 5** zeigt einen Vergleich zwischen den beiden Lösungen und die Vorteile der MSE-Lösung.

Tabelle 5: Cisco 2710 und Cisco MSE im Vergleich

Funktion	Cisco 2710	MSE
Unterstützte Kundenumgebungen	Niedrige Decke für Innenräume (RSSI)	Indoor Low-Decoration (RSSI) Indoor High-Decken (TDOA) Outdoor (TDOA)
Unterstützte Standorttechnologien	Nur RSSI	RSSI-TDOA
Unterstützte Location Engines	Nur Cisco	Cisco Partner-Engine
Max. Anzahl der verfolgten Wi-Fi-Geräte	2,500	18,000
Anzahl unterstützter Services	Einzel (nur Standort)	Mehrere (kontextsensitive Mobilitätslösung, wIPS, künftige Services)
Unterstützte Tags	CCX oder CCX (nur Umfragen)	CCX
Schienen und Regionen	Ja (Clients und Tags)	Ja (nur Clients) Tags - Funktion für AeroScout-Zellen und -Masken
Standortsensoren	Nicht unterstützt	Nicht unterstützt

Kunden mit vorhandenen Cisco 2710-Installationen können ihre Konfiguration auf eine neue Cisco MSE migrieren und beibehalten.

Softwareanforderungen

Die Cisco Aironet Access Points der Serie 1000 für kontextsensitive Software werden nur mit Version 4.2.xxx (xxx>112) unterstützt.

Hinweis: Die Cisco Aironet Access Points der Serie 1000 sind End-of-Life- und End-of-Sale-Produkte. Die Cisco Aironet Access Points der Serie 1000 für die Cisco Context-Aware Solution werden nur von der Version 4.2.xxx (xxx>112) unterstützt. Nur die Cisco Context-Aware Solution der Cisco Mobility Services Engine der Serie 3300 wird unterstützt. Es werden keine anderen Services der Cisco Mobility Services Engine der Serie 3300 unterstützt. Die Cisco Aironet Access Points der Serie 1000 werden von den Versionen 5.x.xxx und künftigen Softwareversionen nicht unterstützt. Kunden wird empfohlen, zu den Cisco Aironet Access Points der Serien 1130, 1140, 1240 oder 1250 zu migrieren, um von den Vorteilen der neuesten Funktionen zu profitieren. Weitere Informationen zu den Ersatzprodukten erhalten Sie von Cisco.

In **Tabelle 6** ist die Softwareversion aufgeführt, die für MSE, WLC und WCS verwendet werden muss. Jede vertikale Spalte stellt kompatible Versionen für MSE, WLC und WCS zusammen dar.

Tabelle 6: Software-Kompatibilitätsmatrix

Service	Systemkomponente	Software-Mindestversion			
		Version	Version	Version	Version
CAS und WPS ¹	MSE	Version 5.1.30.0	Version 5.1.35.0	Version 5.2.91.0	Version 6.0.75.0
	Cisco Wireless LAN Controller (WLC)	Version 4.2: 4.2.130 (oder höher) Version 5.1: 5.1.151.0 (oder höher)	Version 4.2: 4.2.130 (oder höher) Version 5.1: 5.1.163.0 (oder höher)	Version 4.2: 4.2.130 (oder höher) Version 5.2: 5.2.157.0 (oder höher) Version 5.1: 5.1.151.0 (oder höher) oder	Version 4.2: 4.2.130 (oder höher) Version 5.2: 5.2.157.0 (oder höher) Version 5.1: 5.1.151.0 (oder höher) Version 6.0: 6.0.182.0 oder höher Hinweis: Version 5.0.x unterstützt MSE nicht.
	Cisco WCS	Version 5.1: 5.1.64.0 (oder höher)	Version 5.1: 5.1.65.4 (oder höher)	Version 5.2: 5.2.110.0 (oder höher)	Version 6.0: 6.0.132.0 oder höher
	Cisco WCS Navigator	Version 1.3.64.0 (oder höher)	Version 1.3.65.4 (oder höher)	Version 1.4.110.0 (oder höher)	Version 1.4.110.0 (oder höher)

Hinweis: ¹ Version 5.2 ist die Mindestsoftwareanforderung für die Unterstützung von WPS auf dem Controller, dem WCS und der MSE.

Hinweis: Die WCS-Softwareversion muss der MSE-Softwareversion entsprechen, d. h. bei Ausführung von MSE 6.0.x muss WCS ebenfalls 6.0.x sein. Die Lizenzierung wird ab Softwareversion 6.0 durchgesetzt.

Bereitstellungs-Checkliste

Wireless-Planung

- Befolgen Sie die entsprechenden Richtlinien für die Platzierung von Access Points (Standort und Dichte). Sorgen Sie für eine angemessene AP-Perimeterabdeckung. Das WCS Planning Tool kann zur Bestimmung der AP-Dichte und -Platzierung verwendet werden.
- Überprüfen Sie die Wi-Fi-Abdeckung mithilfe des Tools zur Standortuntersuchung und des WCS (Tool zur Standortbereitschaft).
- Überprüfen Sie die Platzierung des Access Points, um Abdeckungslücken zu schließen. Verwenden Sie APs für den Standortoptimierten Überwachungsmodus, um Abdeckungslücken zu schließen.
- Geben Sie an, welche Controller mit welcher MSE über die Seite für die WCS-MSE-Synchronisierung kommunizieren müssen.
- Überprüfen Sie, ob Zertifikate korrekt ausgetauscht werden.

WLC

- Stellen Sie sicher, dass alle APs/Funkmodule betriebsbereit sind und Radio Resource Manager (RRM) aktiviert ist.
- Konfigurieren Sie den NTP-Server auf WLC und MSE, oder synchronisieren Sie beide Geräte (und vorzugsweise WCS) manuell mit der richtigen Zeit- und Zeitzone. **Hinweis:** WLC verwendet GMT(UTC)-Zeit mit der richtigen Zeitzone, um die lokale Zeit abzuleiten. Daher muss die Zeit in UTC eingegeben und die richtige Zeitzone angegeben werden.
- Stellen Sie sicher, dass Clients/Tags vom WLC erkannt werden, indem Sie den Befehl `show [rfid | Client]` *Zusammenfassung*
- Stellen Sie sicher, dass zwischen der MSE und dem Controller ein NMSP mit diesem Befehl auf dem WLC eingerichtet ist, der den `status "nmosp" anzeigt` oder auf dem WCS über **Services > Mobility Services > "MSE" > System > Active Sessions**.
- Überprüfen Sie, ob der WLC mit dem folgenden Befehl die *Zusammenfassung des nmosp-Abonnements* für die richtigen Services abonniert wurde
- Wenn Sie die CCX-Client-Genauigkeit testen, stellen Sie sicher, dass CCX aktiviert ist. `config location plm client enable <interval>` Um die Konfiguration zu überprüfen, verwenden Sie diesen Befehl `show location plm`.
- WLC muss über folgende Standard-nmosp-Parameter verfügen: **Verwendeter Algorithmus:** **Kunde** Timeout für RSSI-Ablaufdatum: 5 Sek. Halbwertszeit: 0 Sek. Schwellenwert benachrichtigen: 0 db **Kalibrierclient** Timeout für RSSI-Ablaufdatum: 5 Sek. Halbwertszeit: 0 Sek. **Nicht autorisierter AP** Timeout für RSSI-Ablaufdatum: 5 Sek. Halbwertszeit: 0 Sek. Schwellenwert benachrichtigen: 0 db **RFID-Tag** Timeout für RSSI-Ablaufdatum: 5 Sek. Halbwertszeit: 0 Sek. Schwellenwert benachrichtigen: 0 db **Konfigurationsbefehl** **Konfigurationsstandort <cmd>** Um diese Werte zu überprüfen **Standortzusammenfassung anzeigen**

WCS/MSE

- Konfigurieren Sie den NTP-Server auf beiden MSE oder synchronisieren Sie beide Geräte (und vorzugsweise WCS) manuell mit der richtigen Zeit- und Zeitzone.

- Stellen Sie sicher, dass Standortberechnungen entweder auf der Nachverfolgungsseite oder auf der MSE-Konsole mit dem Befehl **getserverinfo** erfolgen.
- Stellen Sie mithilfe der Überwachungsfunktion in WCS sicher, dass die WCS-Werte mit den WLC-Werten übereinstimmen.
- Stellen Sie sicher, dass alle APs der Karte zugewiesen sind.
- Die MSE muss mit Netzwerkdesign, WLC(s), kabelgebundenen Switches und Ereignissen synchronisiert werden.
- Stellen Sie sicher, dass die Karten und AP-Positionen zwischen WCS und MSE synchronisiert werden.
- Die Nachverfolgung von Clients/Tags muss in der MSE unter **Dienste > Mobilitätsdienste > <MSE> > Context Aware Service > Administration > Tracking Parameters** aktiviert werden.
- Überprüfen Sie, ob Clients/Tags vom WCS unter **Monitor > Client/Tag** angezeigt werden.
- Wenn Clients und/oder Tags von WCS nicht erkannt werden, stellen Sie sicher, dass die Client/Tag-Lizenzierung auf MSE installiert ist. Stellen Sie außerdem sicher, dass die richtige WCS-Version installiert ist, die Context Aware (WCS PLUS) unterstützt.
- Verwenden Sie das Kalibriertool im WCS, um Signalmerkmale für die jeweilige Umgebung zu kalibrieren.
- Verwenden Sie Standortläufe und -regionen (für die Client-Nachverfolgung) sowie Zellen und Masken (für die Tag-Nachverfolgung), um bestimmte Bereiche auf der Landkarte einzuschließen bzw. auszuschließen, in denen Wi-Fi-Clients nicht angezeigt werden dürfen.
- Überprüfen Sie mit dem Genauigkeitstool in WCS, wie präzise der Standort ist.

Für Clients

- Überprüfen Sie, ob die Nachverfolgung auf MSE aktiviert ist.
- Überprüfen Sie, ob Clients vom WLC erkannt werden.

Für Tags

- Überprüfen Sie, ob die Nachverfolgung auf MSE aktiviert ist.
- Überprüfen Sie, ob Tags vom WLC erkannt werden.
- Die Kanäle 1,6,11 müssen aktiviert sein.
- Die Channel-Wiederholung muss 3 betragen.
- Überprüfen Sie den Akkustatus.

Abschnitt 5: Häufig gestellte technische Fragen

F. Was ist RF-Fingerprinting? Ist es das Gleiche wie RF-Triangulation?

Antwort: RF-Fingerprinting ist eine Methode zur Standortbestimmung mit zwei Schwerpunkten: um zu verstehen, wie Funkwellen in einer bestimmten Umgebung des WLAN interagieren, und um diese Dämpfungsmerkmale auf Geräteinformationen anzuwenden, damit ein Standort bestimmt werden kann. Bei der Triangulation werden Umgebungsvariablen nicht berücksichtigt, sondern es werden nur die Signalstärkemessungen verwendet, um den Gerätestandort zu ermitteln. Beim HF-Fingerprinting werden spezifische Gebäudemerkmale berücksichtigt, da sich diese auf die Übertragung von HF-Signalen und die Genauigkeit der Standortbestimmung auswirken können.

F. Welche Art von Standorttreue kann ich erwarten?

Antwort: Der Standort ist statistischer Natur. Cisco führt die Standortgenauigkeitsspezifikationen

auf maximal zehn Meter 90 % der Zeit und fünf Meter 50 % der Zeit an.

F. Sind die Informationen in Echtzeit?

Antwort: Die Reaktionszeit von Standortinformationen sowie die zugehörigen Clientinformationen sind in erster Linie eine Funktion der Systemverarbeitung. Die Reaktionszeiten können in der Regel zwischen einigen Sekunden und einigen Minuten liegen.

F. Wie skalierbar ist die MSE?

Antwort: Die Cisco MSE 3350 kann bis zu 18.000 Geräte überwachen. Um mehr Geräte zu unterstützen, können dem gleichen System weitere MSEs hinzugefügt werden. Die Obergrenze für simultane Geräte basiert auf der Verarbeitungskapazität der MSE.

F. Wie lange kann ich den Standortverlauf speichern?

Antwort: Der Umfang des Standortverlaufs, den die MSE speichern und wiedergeben kann, ist konfigurierbar. Der Standardwert ist 30 Tage.

F. Wie wirkt sich der Standortdatenverkehr auf mein Netzwerk aus?

Antwort: Der Standortverkehr hängt von der Anzahl der Controller, APs und letztendlich von der Anzahl der Geräte ab, die von einer bestimmten Netzwerkinfrastruktur überwacht werden. Mit zunehmendem Netzwerk wird mehr Datenverkehr von den APs an Wireless-Controller weitergeleitet, die wiederum an die MSE weitergeleitet werden. Der Datenverkehr für eine einzelne Messung ist sehr gering, aber die Anzahl der Messungen hängt von der Anzahl der Geräte und der Häufigkeit der Messungen ab.

F. Wie wird die MSE verwaltet?

Antwort: Bei der Client-Nachverfolgung mit der Context Aware Engine for Clients wird die gesamte Konfiguration und Verwaltung der MSE über das WCS durchgeführt, über die ursprüngliche CLI-Befehlsgesteuerte Einrichtung hinaus. Wenn die Context Aware Engine für Tags verwendet wird (Verfolgung von Tags in Innen- und Außenbereichen bzw. in Außenbereichen), sind Netzverwaltungslösungen von Cisco (WCS) und AeroScout (System Manager) erforderlich.

F. Welche Anforderungen stellt meine Wireless LAN-Architektur an die Unterstützung der MSE?

Antwort: Die MSE funktioniert nur mit einer zentralen Cisco Wireless LAN-Architektur, wie z. B. einer LWAPP-fähigen Infrastruktur. Die korrekte Platzierung der Access Points ist für den Standort unerlässlich. APs müssen sich in der Nähe des Abdeckungsbereichs und intern, wie in diesem Dokument beschrieben, befinden. Siehe Abschnitt **Überlegungen zur Bereitstellung mit vorhandenen Daten- und Sprachdiensten**. WCS mit einer Context Aware Engine-Lizenz ist erforderlich.

F. Worin besteht der Unterschied zwischen dem Standort im WCS und der MSE?

Antwort: Die WCS-Basis gibt an, welcher Access Point ein bestimmtes Gerät erkennen kann, sowie die Signalstärke, bei der das Gerät erkannt wird. WCS mit Location verwendet erweiterte RF-Fingerprinting-Funktionen und kann den Standort eines einzelnen Geräts bedarfsgerecht bestimmen. Die MSE verwendet die gleiche Standortmethode wie das WCS mit Standort, kann jedoch bis zu 18.000 Geräte gleichzeitig verfolgen, wenn sie die Cisco MSE 3350 verwendet. So können Anwendungen von Drittanbietern den Verlauf von Gerätedaten für Anwendungen wie die

Ressourcenverfolgung nutzen.

F. Benötige ich Clientsoftware, um Clients zu finden?

Antwort: Client-Software wird nicht benötigt. Da der Standort direkt in die Wireless-LAN-Infrastruktur integriert ist, hören APs Wi-Fi-Geräte wie gewohnt für Daten-, Sprach- und andere Anwendungen. CCX-Clients werden besser verfolgt als Nicht-CCX-Clients. Cisco empfiehlt daher, CCX-kompatible Clients (v4 oder v5) zu erwerben.

F. Wie lange können Wi-Fi-Tags in Betrieb sein, bevor der Akku ausgetauscht werden muss?

Antwort: Die Lebensdauer eines Tag-Akkus hängt von der Lebensdauer des Akkus eines bestimmten Geräts sowie davon ab, wie oft dieser blinkt oder blinkt. Die Tags können zwischen 100 Tagen und einem Jahr oder sogar länger dauern. Einige Hersteller geben an, dass sie drei bis fünf Jahre lang anhalten können, aber dies hängt von der Beacon-Rate ab.

F. Wie hoch sind die Kosten für Wi-Fi-Tags?

Antwort: Kontaktieren Sie einen Tag-Hersteller. Cisco stellt keine Tags her oder verkauft diese nicht weiter. Tagpreise sind außerdem variabel und abhängig vom Volumen. Diese Tags sind teurer als passive RFID-Tags, da sie eine kontinuierliche Standorttransparenz und wiederverwendbare batteriebetriebene Tags bieten. Sie senden aktiv Signale, die in der Regel größere Reichweiten (mehrere Hundert Meter) bieten und in einer Vielzahl von Formfaktoren mit mehreren Montageoptionen vorliegen. Der Einsatz aktiver RFID-Technik geht im Allgemeinen mit einer kontinuierlichen Verfolgung von mehr mobilen Wertpapieren oder hochgradig haftenden Vermögenswerten im Vergleich zu Gegenständen einher, die im Allgemeinen von passiver RFID verfolgt werden.

[Anhang A: MSE-Einrichtung](#)

Führen Sie diese Schritte aus:

1. **Anmelden:** Melden Sie sich mit den folgenden Anmeldeinformationen an: **root/password**.
2. **Starten des Setup-Prozesses:** Beim erstmaligen Booten fordert die MSE den Administrator auf, das Setup-Skript zu starten. Geben Sie "yes" (Ja) an dieser Eingabeaufforderung ein. **Hinweis:** Wenn die MSE nicht zur Einrichtung auffordert, geben Sie den folgenden Befehl ein:
`/opt/mse/setup/setup.sh`
3. **Konfigurieren Sie den Hostnamen und den DNS-Domännennamen:**

```

Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]: y

The host name should be a unique name that can identify
the device on the network. The hostname should start with
a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

Enter a host name [mse]: MSE-1

Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a domain name for the network domain to which this device
belongs. The domain name should start with a letter, and it should
end with a valid domain name suffix such as ".com". It must contain
only letters, numbers, dashes, and dots.

Enter a domain name: cisco.com

```

4. Konfigurieren der Ethernet-Schnittstellenparameter:

```

Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: 172.20.229.200

Enter the network mask for IP address 172.20.229.200.

Enter network mask [255.255.255.0]: 255.255.255.0

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from
the first ethernet interface.

Enter default gateway address [1.1.1.1]: 172.20.229.1

```

Wenn Sie zur Eingabe der Schnittstellenparameter "eth1" aufgefordert werden, geben Sie **Überspringen ein**, um mit dem nächsten Schritt fortzufahren, da für den Betrieb keine zweite NIC erforderlich ist. **Hinweis:** Die konfigurierte Adresse muss IP-Verbindungen zu den potenziellen Wireless LAN-Controllern und dem mit dieser Appliance verwendeten WCS-Managementssystem bereitstellen.

5. DNS-Server-Informationen eingeben: Für eine erfolgreiche Domänenauflösung ist nur ein DNS-Server erforderlich. Geben Sie für Ausfallsicherheit Backup-Server ein.

```

Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enable DNS (yes/no) [yes]: y
Enter primary DNS server IP address: 172.20.229.10
Enter backup DNS server IP address (or none) [none]: 172.20.229.20
Enter another backup DNS server IP address (or none) [none]:

```

6. Zeitzone konfigurieren: Wenn die standardmäßige Zeitzone von New York nicht für Ihre Umgebung anwendbar ist, können Sie sie in den Standortmenüs richtig einstellen.

```

Current timezone=[America/New_York]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean

```

7. **NTP oder Systemzeit konfigurieren:** NTP ist optional, stellt jedoch sicher, dass Ihr System die korrekte Systemzeit erhält. Wenn Sie "Nein" auswählen, werden Sie aufgefordert, die aktuelle Uhrzeit für das System festzulegen.

```

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select. Otherwise,
you will be prompted to enter the current date and time.

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select. Otherwise,
you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: yes
Enter NTP server name or address: time.nist.gov
Enter another NTP server IP address (or none) [none]:

```

Hinweis: Es ist zwingend erforderlich, dass die richtige Zeit für die Mobility Services Engine, den Wireless LAN Controller und das WCS Management System festgelegt wird. Dies ist möglich, wenn Sie alle drei Systeme auf denselben NTP-Server verweisen und sicherstellen, dass die richtigen Zeitzonen konfiguriert sind.

8. **Root-Anmeldung der lokalen Konsole aktivieren:** Dieser Parameter wird verwendet, um den lokalen Konsolenzugriff auf das System zu aktivieren/deaktivieren. Dies muss aktiviert sein, damit eine lokale Fehlerbehebung möglich ist.

```

Remote root login is currently disabled.
Configure remote root access? (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to allow
remote root login via secure shell for this machine.

Enable remote root login (yes/no) [no]: yes

```

9. **SSH-Root-Anmeldung (Secure Shell) aktivieren: Optional:** Dieser Parameter wird verwendet, um den Remote-Konsolenzugriff auf das System zu aktivieren/deaktivieren. Diese Option muss aktiviert sein, damit eine Remote-Fehlerbehebung möglich ist. Sicherheitsrichtlinien des Unternehmens können jedoch vorschreiben, dass Sie diese Option deaktivieren.


```
SSH root access is currently disabled.
Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to enable ssh
root login. If you disable this option, only console
root login will be possible.

Enable ssh root access (yes/no): yes
```

10. Konfigurieren des Modus für einen Benutzer und der Kennwortstärke: Diese Konfigurationsparameter sind nicht erforderlich, und die Standardeinstellung ist, diese zu überspringen, die Eingabe von "s".

```
Single user mode password check is currently disabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]: s

Login and password strength related parameter setup
Maximum number of days a password may be used : 99999
Minimum number of days allowed between password changes : 0
Minimum acceptable password length : 5
Login delay after failed login :
Checking for strong passwords is currently disabled.
Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Skip]:
s
```

11. Anmeldebanner festlegen: Ein Anmeldebanner informiert Benutzer über die Verwendung des Systems und warnt vor dem Zugriff unbefugter Benutzer auf das System. Da es sich bei dem Anmeldebanner um eine mehrzeilige Nachricht handeln kann, beendet ein einzelner Punkt (.) die Nachricht und fährt mit dem nächsten Schritt fort.

```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]: yes

Enter text to be displayed as login banner. Enter a single period
on a line to terminate.

Login banner [Cisco Mobility Service Engine]:
MSE-1
Unauthorized Access is not allowed
.
```

12. Ändern des Root-Kennworts: Dieser Schritt ist zur Gewährleistung der Systemsicherheit unerlässlich. Wählen Sie unbedingt ein sicheres Kennwort aus Buchstaben und Zahlen ohne Wörterbuchwörter. Die Mindestlänge für das Kennwort beträgt 8 Zeichen.

```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a password for the superuser.

Enter root password:
Confirm root password:
```

13. Konfigurieren eines GRUB-Kennworts: Optional: Dieser Konfigurationsparameter ist nicht erforderlich. Die Standardeinstellung zum Überspringen lautet "s".

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]: s
```

14. Konfigurieren eines WCS-Kommunikationskennworts.

```

Configure WCS communication password? (Y)es/(S)kip/(U)se default [Skip]: yes
Enter a password for the admin user.
The admin user is used by the WCS and other northbound systems
to authenticate their SOAP/XML session with the server.
Once this password is updated, it must correspondingly be updated
on the WCS page for MSE General Parameters so that the WCS can
communicate with the MSE.

Enter WCS communication password: 
Confirm WCS communication password: 

```

15. **Änderungen speichern und neu starten:** Wenn das Setup-Skript abgeschlossen ist, speichern Sie die Änderungen, wenn Sie dazu aufgefordert werden. Folgen Sie nach dem Speichern den Anweisungen, um die MSE neu zu starten und sicherzustellen, dass alle Einstellungen erfolgreich angewendet werden.
16. **Starten des MSE-Service:** Melden Sie sich mit dem zuvor in Schritt 12 konfigurierten Benutzernamen root und Kennwort bei der MSE an. Führen Sie den Befehl **service msed start** aus, um den MSE-Dienst zu starten.

```

login as: root
Cisco Mobility Service Engine

root@172.20.226.203's password: 
Last login: Wed Jul 23 10:11:58 2008 from dhcp-171-71-123-7.cisco.com
[root@MSE-1 ~]# service msed start
Starting MSE Platform
Cannot find UDI information. Exiting
null
Invalid Platform type. Now Exiting.
Starting MSE Platform, waiting to check the status.
Starting MSE Platform, waiting to check the status.
MSE Platform is up, getting the status

```

17. **Aktivieren Sie den MSE-Dienst, um beim Start zu starten:** Führen Sie den Befehl **chkconfig** aus.

MSE zum WCS hinzufügen

Führen Sie diese Schritte aus:

1. **Rufen Sie die Seite für die Konfiguration von Mobilitätsdiensten auf:** Melden Sie sich bei WCS an, und klicken Sie im Dropdown-Menü "Mobility" (Mobilität) auf **Mobility Services**.



2. **Hinzufügen der Mobility Services Engine zum WCS:** Wählen Sie aus dem Dropdown-Menü rechts die Option **Engine für Mobilitätsdienste hinzufügen** aus, und klicken Sie auf **Weiter**. Geben Sie einen eindeutigen Gerätenamen für die MSE, die zuvor im MSE-Setup konfigurierte IP-Adresse, einen Kontaktnamen für den Support und das bei der MSE-

Einrichtung konfigurierte WCS-Kommunikationskennwort ein. Ändern Sie den Benutzernamen nicht von der Standardeinstellung **admin**.

Mobility Services Engine > General Properties > New

General

Device Name	<input type="text" value="MSE Demo"/>
IP Address	<input type="text" value="172.20.226.199"/>
Contact Name	<input type="text" value="MSE Support Contact"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>

3. Wählen Sie den auf der MSE auszuführenden kontextsensitiven Dienst aus.

Mobility Services

Admin Status	Name
<input checked="" type="checkbox"/>	Context Aware Service
<input type="checkbox"/>	Wireless Intrusion Protection Service

4. Synchronisieren: Stellen Sie sicher, dass Sie **Netzwerkdesigns, Controller und Ereignisgruppen** synchronisieren.

Mobility Services Engine Added > 'MSE Demo'

WCS contains data, please go to the Synchronize page to push data to the Mobility Services Engine.

Please synchronize the following Controllers

WLC-1

Go to Synchronize...

Mobility Services > Synchronize WCS and MSE(s)

Network Designs **Controllers** Event Groups

Devices [Mobility Services]	Controllers	Sync. Status	Message
MSE Demo [W]	-- None Assigned --		Assign

5. **Zu synchronisierende Controller:** Es wird ein Popup mit einer Liste von Controllern angezeigt, mit denen die MSE synchronisiert werden soll. Wählen Sie die gewünschten Controller für die Synchronisierung aus, und klicken Sie auf **OK**.



Controller Name	Controller IP Address	Version	Supported Services	Currently Assigned To
<input checked="" type="checkbox"/> WLC-1	172.20.226.197	5.2.72.0	[C, W, M]	

OK **Cancel**

Wenn das Popup-Fenster geschlossen wurde, klicken Sie unten im Dialogfeld "Synchronisieren von WCS und MSE(s)" auf **Synchronisieren**. **Hinweis:** Der Cisco Context Aware Service ist in hohem Maße von einer synchronisierten Uhr zwischen dem Wireless LAN Controller, dem WCS und der MSE abhängig. Wenn alle drei Systeme nicht auf denselben NTP-Server zeigen und mit denselben Zeitzoneneinstellungen konfiguriert sind, funktioniert die kontextsensitive Funktion nicht korrekt. Bevor Sie versuchen, eine Fehlerbehebung durchzuführen, stellen Sie sicher, dass die Systemuhr für alle Komponenten des kontextsensitiven Systems identisch ist.

Anhang B: WLC- und MSE-Befehle

WLC-Befehle

```

config location expiry ?
client          Timeout for clients
calibrating-client Timeout for calibrating clients
tags           Timeout for RFID tags
rogue-aps      Timeout for Rogue APs
  
```

show location ap-detect ?

all Display all (client/rfid/rogue-ap/rogue-client) information
client Display client information
rfid Display rfid information
rogue-ap Display rogue-ap information
rogue-client Display rogue-client information
(Cisco Controller) >show location ap-detect client

show client summary

Number of Clients..... 7
MAC Address AP Name Status WLAN/Guest-Lan Auth Protocol Port Wired

00:0e:9b:a4:7b:7d AP6 Probing N/A No 802.11b 1 No
00:40:96:ad:51:0c AP6 Probing N/A No 802.11b 1 No
(Cisco Controller) >show location summary

Location Summary
Algorithm used: Average
Client
RSSI expiry timeout: 5 sec
Half life: 0 sec
Notify Threshold: 0 db
Calibrating Client
RSSI expiry timeout: 5 sec
Half life: 0 sec
Rogue AP
RSSI expiry timeout: 5 sec
Half life: 0 sec
Notify Threshold: 0 db
RFID Tag
RSSI expiry timeout: 5 sec
Half life: 0 sec
Notify Threshold: 0 db

show rfid config

RFID Tag data Collection..... Enabled
RFID timeout..... 1200 seconds
RFID mobility..... Oui:00:14:7e : Vendor:pango State:Disabled

(Cisco Controller) >config location ?

plm Configure Path Loss Measurement (CCX S60) messages
algorithm Configures the algorithm used to average RSSI and SNR values
notify-threshold Configure the LOCP notification threshold for RSSI measurements
rssi-half-life Configures half life when averaging two RSSI readings
expiry Configure the timeout for RSSI values

config location expiry client ?

<seconds> A value between 5 and 3600 seconds

config location rssi-half-life client ?

<seconds> Time in seconds (0,1,2,5,10,20,30,60,90,120,180,300 sec)

show nmsp subscription summary

Mobility Services Subscribed:
Server IP Services

172.19.32.122 RSSI, Info, Statistics, IDS

MSE-Befehle

to determine status of MSE services
[root@MSE ~]# getserverinfo

to start Context Aware engine for client tracking

```
[root@MSE ~]# /etc/init.d/mseed start
```

to determine status of Context Aware engine for client tracking

```
[root@MSE ~]# /etc/init.d/mseed status
```

to stop Context Aware engine for client tracking

```
[root@MSE ~]# /etc/init.d/mseed stop
```

diagnostics command

```
[root@MSE ~]# rundia
```

Hinweis: Mit dem Befehl **rundia** können auch MSE UDI-Informationen angezeigt werden, die zum Abrufen der Lizenzdatei für Context Aware Engine für Clients erforderlich sind.

Anhang C: MSE-Upgrade von 5.x auf 6.0

Führen Sie diese Schritte aus:

1. Sichern Sie die MSE-Datenbank vor der Version 6.x aus dem WCS. zu diesem Link navigieren: **Service > Mobilitätsdienste > Wählen Sie MSE > Wartung > Backup** aus.
2. Um Daten und Konfigurationen für Tags zu sichern, folgen Sie der [AeroScout-Dokumentation](#)
3. 6.x-Image von WCS auf MSE herunterladen zu diesem Link navigieren: **Services > Mobility Service > Wählen Sie MSE** aus, und klicken Sie dann im linken Bereich auf **Maintenance > Download Software**, wählen Sie das MSE-Image von Ihrem PC aus, und klicken Sie auf **Download**. Nach dem Herunterladen wird das MSE-Image automatisch entzippt und in den Ordner `/opt/installers` der MSE eingefügt. Sie müssen das Image manuell über die MSE-CLI installieren.

Transfer Software Image

Select from uploaded images to transfer into the Server

AIR-LOC2700-L-K9-3-1-38-0.bin.gz

Browse a new software image to transfer into the Server

Timeout 1 - 999999 secs

4. Führen Sie diesen Befehl aus, um das MSE-Framework zu beenden: `/etc/init.d/mseed stop`.
5. Geben Sie in der MSE-Konsole `cd /opt/installers` aus. In diesem Verzeichnis sehen Sie die Datei, die Sie in Schritt 3 heruntergeladen haben. Das Verzeichnis sieht wie folgt aus:

```
[root@heitz-3350 installers]# cd /opt/installers
[root@heitz-3350 installers]# ls
CISCO-MSE-L-K9-6-0-73-0-64bit.bin  diagnostics.log
```

```
CISCO-MSE-L-K9-6-0-75-0-64bit.bin MSE_6_0_70_0.bin  
[root@heitz-3350 installers]#
```

6. Um das MSE-Image zu installieren, führen Sie die Datei aus und befolgen Sie die Anweisungen:

```
[root@heitz-3350 installers]# ./CISCO-MSE-L-K9-6-0-73-0-64bit.bin
```

Hinweis: Die Warnmeldung für Lizenzanforderungen an MSE zur Nachverfolgung von Elementen wird sofort mit der Version 6.0 MR1 angezeigt. Diese Warnmeldung wird auch am Ende nach Abschluss der Installation angezeigt. Mit der Version 6.0 wird diese Meldung erst am Ende angezeigt, nachdem die Installation abgeschlossen ist. Eine Vorabwarnung wurde mit 6.0 MR1 hinzugefügt, um Benutzer auf die Durchsetzung von Lizenzen hinzuweisen. Die Meldung sieht wie folgt aus: "Die Lizenzierung auf der Mobility Services Engine wird mit dieser Softwareversion durchgesetzt. Stellen Sie sicher, dass Sie den Produktautorisierungsschlüssel (PAK) zur Verfügung haben, und beachten Sie die Anweisungen im PapierPAK-Zertifikat und im MSE-Benutzerhandbuch, um die Lizenzierung für das System zu aktivieren." Bei der Ausführung der Datei hat der Benutzer die Möglichkeit, die Datenbank zu behalten oder zu entfernen.

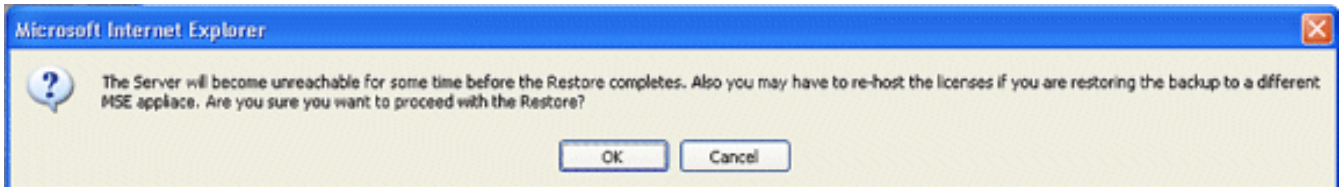
7. Führen Sie nach der Installation des Images diesen Befehl aus, um das MSE-Framework zu starten: **/etc/init.d/msed start**.
8. Die MSE verwendet ab sofort die Evaluierungslizenzen, die im Lieferumfang der 6.0-Softwareversion enthalten sind.
9. Fügen Sie die permanente Lizenz hinzu, die Sie erhalten haben, indem Sie eine PAK-Nummer von WCS registrieren. zu diesem Link navigieren: **Administration > License Center > Files > MSE Files > Add**. Wählen Sie MSE aus dem Dropdown-Menü aus, suchen Sie nach der Lizenzdatei auf Ihrem PC, und laden Sie sie hoch.
10. MSE-Dienste werden nach dem Hochladen der Lizenz auf die MSE neu gestartet. Warten Sie also einige Minuten, bevor Sie einen anderen Vorgang ausführen. Erhalten Sie den MSE-Status, wenn Sie den Befehl **/etc/init.d/msed status** ausgeben.
11. Wenn Sie bei der Installation des MSE-Images die Datenbankoption wie in Schritt 6 beibehalten möchten, müssen Sie die zuvor gesicherte Datenbank (für Clients und Tags) nicht wiederherstellen. Andernfalls müssen Sie die MSE-Datenbank wiederherstellen. Navigieren Sie zu **Service > Mobility Services**, wählen Sie **MSE** im linken Bereich Maintenance aus, und klicken Sie auf **Restore (Wiederherstellen)**. **Hinweis:** Um Tag-Informationen wiederherzustellen, folgen Sie der [AeroScout-Dokumentation](#) .

Anhang D: MSE-Datenbankwiederherstellung

Die MSE DB kann auf drei verschiedene Arten wiederhergestellt werden:

- **Option 1:** Wenn Sie das MSE-Image auf 6.0 aktualisieren, sollten Sie fortfahren, wenn das Installationsprogramm feststellt, dass die MSE bereits ausgeführt wird. Die Meldung zeigt Folgendes: "Auf dem System scheint bereits eine Cisco Mobility Services Engine installiert zu sein. Wenn Sie **Weiter** wählen, werden alle aktuell installierten Komponenten dauerhaft entfernt (nur Datenbank- und Lizenzdateien bleiben erhalten)."
- **Option 2:** Bei der Deinstallation des MSE-Images stehen Ihnen zwei Optionen zur Verfügung. Die erste Option besteht darin, die Datenbank zu behalten, und die zweite Option besteht darin, die Datenbank zu entfernen. Wenn die Datenbank gespeichert wird, ist keine manuelle Wiederherstellung erforderlich. Wenn die Datenbank entfernt wird, folgen Sie der dritten Option.

- **Option 3:**Führen Sie eine Neuinstallation durch, d. h. Sie nehmen entweder ein neues MSE-Feld mit einem Image vor 6.0 oder eine MSE, bei der die Datenbank entfernt ist. Sie müssen die gesicherte Datenbank wiederherstellen (siehe Option 1 zu MSE mit 6.0). Wenn das gesicherte MSE-Image auf einer anderen MSE wiederhergestellt wurde, muss die Lizenz neu gehostet werden, damit sie auf der aktuellen MSE verwendet werden kann. MSE-Lizenzen sind an MSE UDI gebunden. Innerhalb der Wiederherstellung erhält der Benutzer eine Meldung in WCS: "Sie müssen die Lizenzen möglicherweise neu hosten, wenn Sie die Sicherung auf einer anderen MSE-Appliance wiederherstellen."



Zugehörige Informationen

- [Cisco 3350 Mobility Services - Erste Schritte](#)
- [Cisco 3310 Mobility Services Engine - Erste Schritte](#)
- [Cisco Mobility Services Engine - Implementierungsleitfaden für kontextsensitive Mobilitätslösungen](#)
- [Häufig gestellte Fragen zu Mobilitätsgruppen](#)
- [Wi-Fi Location-Based Services 4.1 Designleitfaden](#)
- [Cisco Context-Aware Service Configuration Guide, Version 6.0](#)
- [Lizenzierungs- und Bestellanleitung für die Cisco Mobility Services Engine der Serie 3300](#)
- [Konfigurationsleitfaden für Cisco Wireless LAN Controller](#)
- [RFID-Tags, eine genauere Betrachtung der RFID-Tags und ihrer Konfiguration](#)
- [Cisco Aironet-Antennen und -Zubehör - Referenzhandbuch](#)
- [AeroScout-Unterstützung](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)