Erkennung nicht autorisierter APs unter Unified Wireless Networks

Inhalt

Einführung

Drahtlose Netzwerke erweitern kabelgebundene Netzwerke und erhöhen die Mitarbeiterproduktivität und den Informationszugriff. Ein nicht autorisiertes Wireless-Netzwerk stellt jedoch zusätzliche Sicherheitsbedenken dar. Die Port-Sicherheit in kabelgebundenen Netzwerken ist weniger wichtig, und Wireless-Netzwerke stellen eine einfache Erweiterung für kabelgebundene Netzwerke dar. Daher kann ein Mitarbeiter, der seinen eigenen Cisco Access Point (AP) in eine gut gesicherte Wireless- oder kabelgebundene Infrastruktur einbindet und unbefugten Benutzern den Zugriff auf dieses sonst gesicherte Netzwerk ermöglicht, leicht ein sicheres Netzwerk gefährden.

Durch die Erkennung nicht autorisierter APs kann der Netzwerkadministrator diese Sicherheitsbedenken überwachen und beseitigen. Die Cisco Unified Network-Architektur bietet zwei Methoden zur Erkennung von unberechtigten Benutzern, die eine vollständige Identifizierung und Eindämmung von Bedrohungen ermöglichen, ohne dass teure und schwer zu rechtfertigende Overlay-Netzwerke und -Tools erforderlich sind.

Übersicht der Funktionen

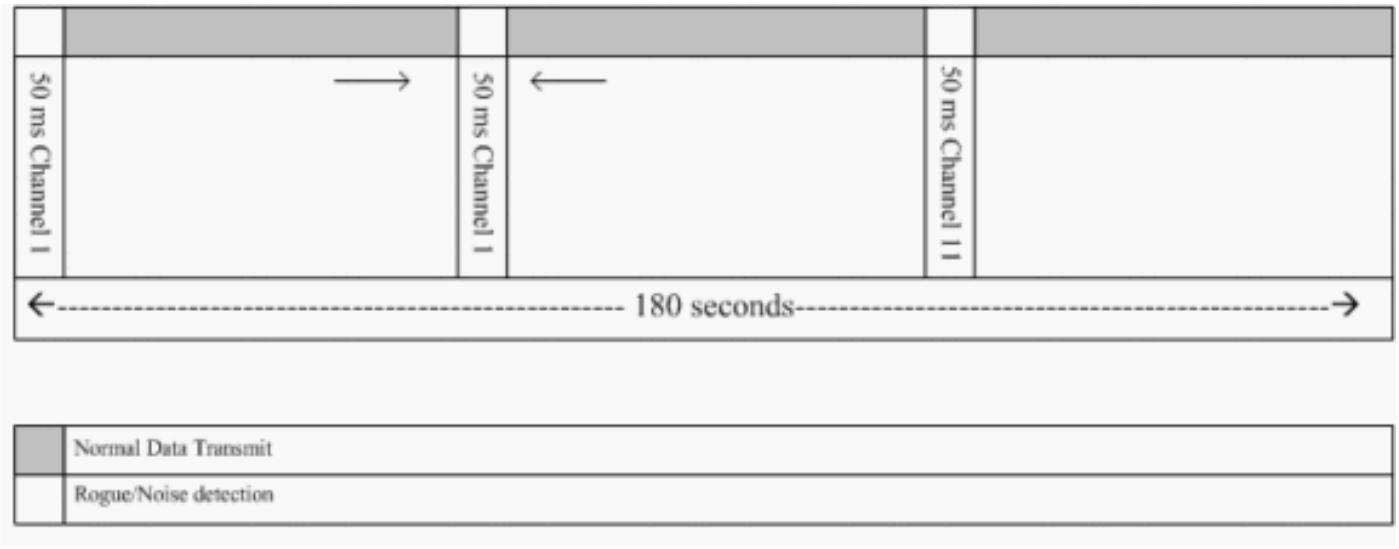
Die Erkennung von nicht autorisierten Objekten ist nicht an irgendwelche Vorschriften gebunden und es ist keine rechtliche Einhaltung für deren Betrieb erforderlich. Bei der Eindämmung von sicherheitsgefährdenden Praktiken treten jedoch in der Regel rechtliche Probleme auf, die den Infrastrukturanbieter in eine unangenehme Lage versetzen können, wenn er automatisch in Betrieb genommen wird. Cisco ist sehr sensibel auf solche Probleme und bietet diese Lösungen an. Jeder Controller ist mit einem RF-Gruppennamen konfiguriert.Sobald ein einfacher Access Point bei einem Controller registriert ist, wird ein **Authentifizierungsinformationselement (IE)** eingebettet, das für die auf dem Controller konfigurierte RF-Gruppe in allen ihren Beacons/Sonde-

Response-Frames spezifisch ist. Wenn der Access Point Beacons/Sonde-Response-Frames von einem Access Point entweder ohne diesen **IE** oder mit **falschem IE** hört, meldet der Lightweight Access Point, dass der Access Point ein unberechtigter Access Point ist, zeichnet seine BSSID in einer nicht autorisierten Tabelle auf und sendet die Tabelle an den Controller. Es gibt zwei Methoden, nämlich das Rogue Location Discovery Protocol (RLDP) und den passiven Betrieb, die ausführlich erläutert werden. Siehe den Abschnitt Bestimmen aktiver Schurken.

Erkennung nicht autorisierter Infrastrukturen

Die Erkennung von nicht autorisierten Zugriffen in einer aktiven Wireless-Umgebung kann kostspielig sein. Bei diesem Prozess wird der Access Point aufgefordert, den Dienst einzustellen, auf Geräusche zu achten und unberechtigte Zugriffe zu erkennen. Der Netzwerkadministrator konfiguriert die zu scannenden Kanäle und konfiguriert den Zeitraum, in dem alle Stationen gescannt werden. Der Access Point überwacht 50 ms auf unberechtigte Client-Beacons und kehrt dann zum konfigurierten Kanal zurück, um die Clients erneut zu warten. Diese aktive Prüfung identifiziert in Verbindung mit Nachbar-Meldungen, welche APs unautorisiert sind und welche APs gültig sind und Teil des Netzwerks sind. Um die gescannten Kanäle und den Scanzeitraum zu konfigurieren, gehen Sie zu **Wireless > 802.11b/g Network** (entweder "**b/g**" oder "**a**" je nach Netzwerkanforderungen), und wählen Sie die **Auto RF**-Schaltfläche in der oberen rechten Ecke des Browserfensters aus.

Sie können nach unten zu **Noise/Interference/Rogue Monitoring Channels** scrollen, um die zu scannenden Kanäle auf unberechtigte oder laute Kanäle zu konfigurieren. Folgende Optionen stehen zur Auswahl: Alle Kanäle (1 bis 14), Länderkanäle (1 bis 11) oder Dynamic Channel Association (DCA) Channels (standardmäßig 1, 6 und 11). Die Scandauer über diese Kanäle kann im gleichen Fenster unter **Überwachungsintervall (60 bis 3600 Sekunden)** zusammen mit dem Rauschmessintervall konfiguriert werden. Standardmäßig beträgt das Abhörintervall für Off-Channel-Rauschen und unberechtigte Geräte 180 Sekunden. Das bedeutet, dass jeder Kanal alle 180 Sekunden gescannt wird. Dies ist ein Beispiel für die DCA-Kanäle, die alle 180 Sekunden gescannt werden:



Wie gezeigt, lässt eine große Anzahl von Kanälen, die für das Scannen konfiguriert sind, in Verbindung mit den kurzen Scanintervallen weniger Zeit für den AP, um Daten-Clients zu bedienen.

Der Lightweight Access Point wartet, um Clients und APs als unberechtigte Personen zu bezeichnen, da diese unberechtigten Personen möglicherweise erst nach Abschluss eines

weiteren Zyklus von einem anderen Access Point gemeldet werden. Derselbe AP wechselt erneut zum gleichen Kanal, um unberechtigte APs und Clients sowie Störungen und Interferenzen zu überwachen. Wenn dieselben Clients und/oder APs erkannt werden, werden sie auf dem Controller erneut als unberechtigte Personen aufgelistet. Der Controller beginnt nun zu ermitteln, ob diese unberechtigten Geräte an das lokale Netzwerk oder einfach an einen benachbarten Access Point angeschlossen sind. In beiden Fällen gilt ein Access Point, der nicht Teil des verwalteten lokalen Wireless-Netzwerks ist, als nicht autorisiert.

Details zu nicht autorisierten Benutzern

Ein Lightweight Access Point geht 50 ms lang außer Kanal, um unberechtigte Clients zu überwachen, Rauschen zu überwachen und Kanalstörungen zu erkennen. Alle erkannten nicht autorisierten Clients oder APs werden an den Controller gesendet, der folgende Informationen sammelt:

- Nicht autorisierte AP-MAC-Adresse
- Der unberechtigte AP-Name
- MAC-Adresse des bzw. der nicht autorisierten verbundenen Clients
- Legt fest, ob die Frames mit WPA oder WEP geschützt sind.
- Präambel
- Signal-Rausch-Verhältnis (SNR)
- Signalstärke-Indikator des Empfängers (RSSI)

Access Point mit Erkennung nicht autorisierter Geräte

Sie können festlegen, dass ein Access Point als unberechtigter Detektor fungiert, der es auf einen Trunk-Port platziert, sodass er alle mit dem Kabel verbundenen VLANs hören kann. Der Client wird dann im kabelgebundenen Subnetz aller VLANs gefunden. Der nicht autorisierte Detektor-AP überwacht ARP-Pakete (Address Resolution Protocol), um die Layer-2-Adressen identifizierter nicht autorisierter Clients oder nicht autorisierter APs zu ermitteln, die vom Controller gesendet werden. Wenn eine Layer-2-Adresse gefunden wird, die übereinstimmt, generiert der Controller einen Alarm, der den nicht autorisierten Access Point oder Client als Bedrohung identifiziert. Dieser Alarm weist darauf hin, dass das nicht autorisierte Gerät im kabelgebundenen Netzwerk erkannt wurde.

Bestimmen aktiver Schurken

Nicht autorisierte APs müssen zweimal "erkannt" werden, bevor sie vom Controller als unberechtigtes Gerät hinzugefügt werden. Nicht autorisierte APs gelten nicht als Bedrohung, wenn sie nicht mit dem kabelgebundenen Segment des Unternehmensnetzwerks verbunden sind. Um festzustellen, ob das Schurke aktiv ist, werden verschiedene Ansätze verwendet. Zu diesen Ansätzen gehört auch die RLDP.

RLDP (Rogue Location Discovery Protocol)

RLDP ist ein aktiver Ansatz, der verwendet wird, wenn nicht autorisierte APs keine Authentifizierung (offene Authentifizierung) konfiguriert haben. Dieser Modus, der standardmäßig deaktiviert ist, weist einen aktiven Access Point an, in den unautorisierten Kanal zu wechseln und eine Verbindung zum unberechtigten Gerät als Client herzustellen. Während dieser Zeit sendet der aktive Access Point deauthentifizierungsmeldungen an alle angeschlossenen Clients und

beendet dann die Funkschnittstelle. Anschließend wird er dem nicht autorisierten Access Point als Client zugeordnet.

Der Access Point versucht dann, eine IP-Adresse vom nicht autorisierten Access Point zu erhalten, und leitet ein User Datagram Protocol (UDP)-Paket (Port 6352), das den lokalen Access Point und unberechtigte Verbindungsinformationen enthält, über den nicht autorisierten Access Point an den Controller weiter. Wenn der Controller dieses Paket empfängt, wird der Alarm so eingerichtet, dass er den Netzwerkadministrator darüber informiert, dass ein nicht autorisierter Access Point im kabelgebundenen Netzwerk mit der RLDP-Funktion erkannt wurde.

Hinweis: Verwenden Sie den Befehl **debug dot11 rldp enable**, um zu überprüfen, ob der Lightweight Access Point eine DHCP-Adresse vom nicht autorisierten Access Point zuordnet und empfängt. Mit diesem Befehl wird auch das vom Lightweight Access Point an den Controller gesendete UDP-Paket angezeigt.

Ein Beispiel für ein vom Lightweight AP gesendetes UDP-Paket (Ziel-Port 6352) wird hier angezeigt:

```
0020 0a 01 01 0d 0a 01 .......(..*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
......x........ 0040 00 00 00 00 00 00 00 00 00 00
```

Die ersten 5 Byte der Daten enthalten die DHCP-Adresse, die der nicht autorisierte Access Point dem lokalen Modus-AP gibt. Die nächsten 5 Byte sind die IP-Adresse des Controllers, gefolgt von 6 Byte, die die nicht autorisierte AP-MAC-Adresse darstellen. Dann gibt es 18 Byte Nullen.

Passiver Betrieb:

Dieser Ansatz wird verwendet, wenn nicht autorisierte APs eine Authentifizierung aufweisen, entweder WEP oder WPA. Wenn eine Authentifizierung auf einem nicht autorisierten Access Point konfiguriert wird, kann der Lightweight Access Point keine Verbindung herstellen, da er den auf dem nicht autorisierten Access Point konfigurierten Schlüssel nicht kennt. Der Prozess beginnt mit dem Controller, wenn er die Liste der nicht autorisierten Client-MAC-Adressen an einen AP weiterleitet, der als nicht autorisierter Detektor konfiguriert ist. Der unberechtigte Detektor scannt alle angeschlossenen und konfigurierten Subnetze auf ARP-Anfragen, und ARP sucht nach einer übereinstimmenden Layer-2-Adresse. Wenn eine Übereinstimmung erkannt wird, benachrichtigt der Controller den Netzwerkadministrator, dass ein unberechtigter Fehler im kabelgebundenen Subnetz erkannt wird.

Active Rogue Containment

Sobald ein nicht autorisierter Client im kabelgebundenen Netzwerk erkannt wird, kann der Netzwerkadministrator sowohl den nicht autorisierten Access Point als auch die nicht autorisierten Clients enthalten. Dies ist möglich, da 802.11-De-Authentifizierungspakete an Clients gesendet werden, die mit nicht autorisierten APs verbunden sind, sodass die Bedrohung, die durch eine solche Lücke entsteht, verringert wird. Jedes Mal, wenn versucht wird, den nicht autorisierten Access Point einzudämmen, werden fast 15 % der Ressourcen des Lightweight Access Point verwendet. Daher wird empfohlen, den nicht autorisierten Access Point physisch zu lokalisieren und zu entfernen, sobald er enthalten ist.

Hinweis: Nach der Erkennung des Routers in der WLC-Version 5.2.157.0 können Sie nun festlegen, dass der erkannte nicht autorisierte Router entweder manuell oder automatisch enthalten wird. In Controller-Softwareversionen vor 5.2.157.0 ist die manuelle Eingrenzung die

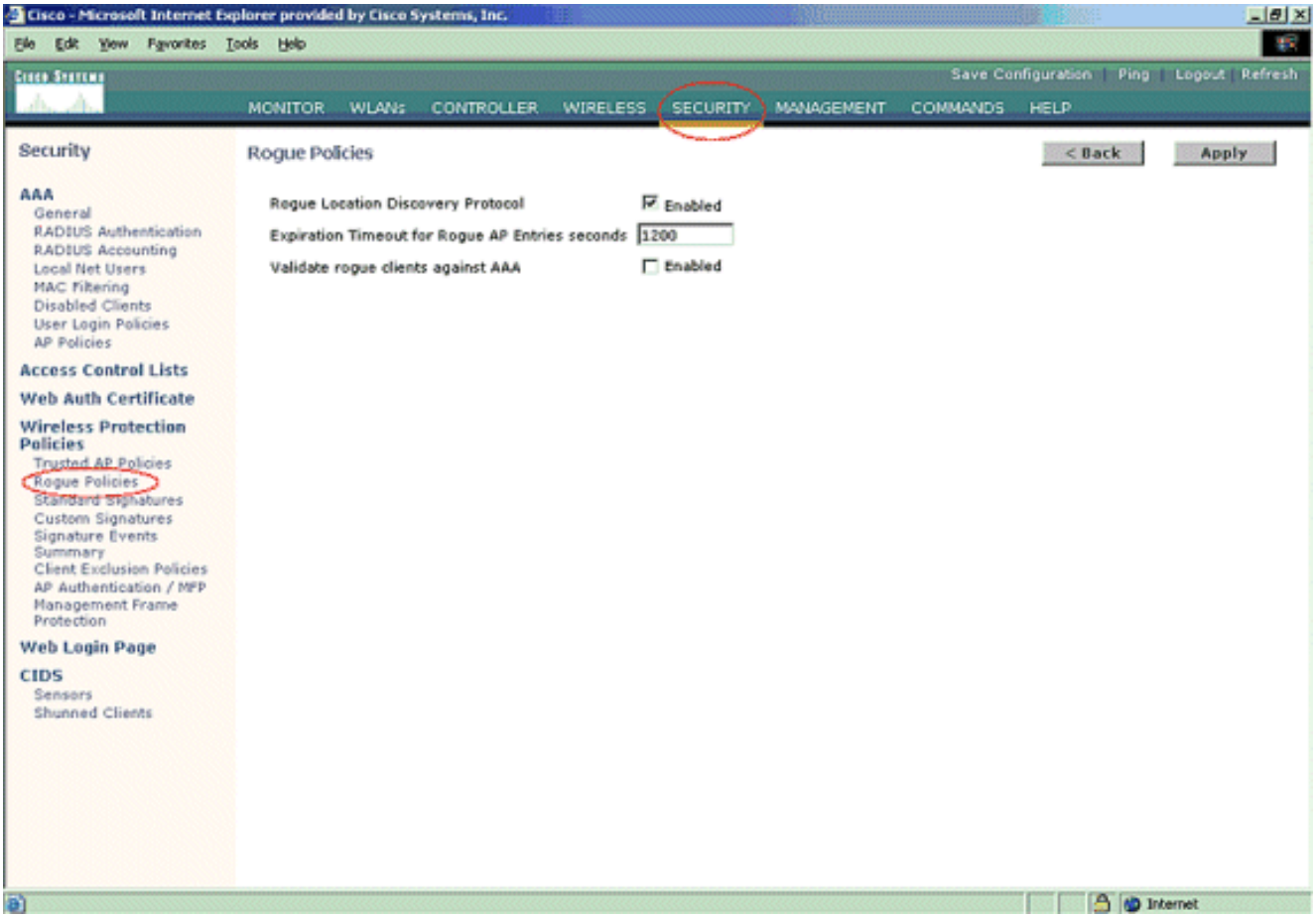
einzige Option.

Erkennung nicht autorisierter APs - Konfigurationsschritte

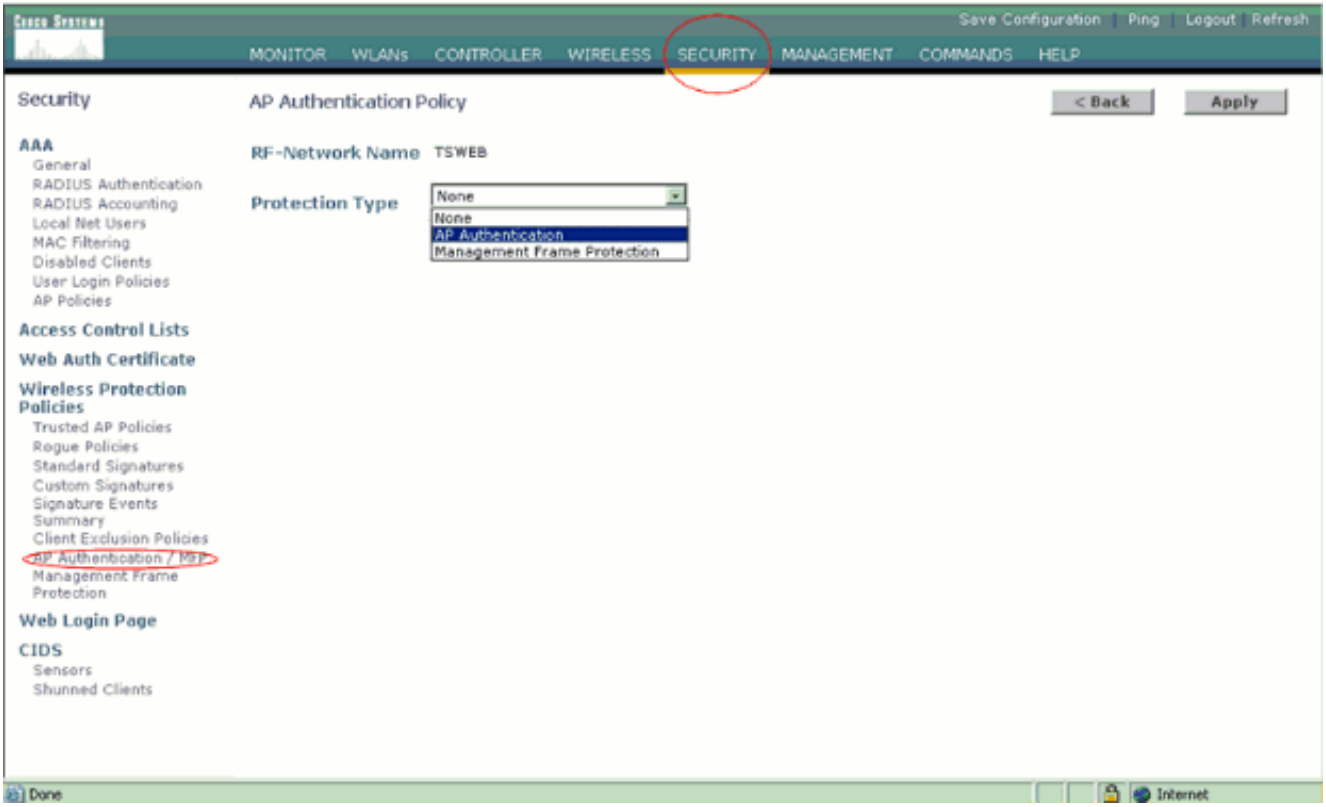
Fast die gesamte Konfiguration zur Erkennung von unautorisierten Zugriffen ist standardmäßig aktiviert, um eine maximale, sofort einsatzbereite Netzwerksicherheit zu ermöglichen. Bei diesen Konfigurationsschritten wird davon ausgegangen, dass auf dem Controller keine Erkennung von unberechtigten Geräten eingerichtet wurde, um wichtige Informationen zur Erkennung von Sicherheitsrisiken zu klären.

Gehen Sie wie folgt vor, um die Erkennung von unberechtigten Benutzern einzurichten:

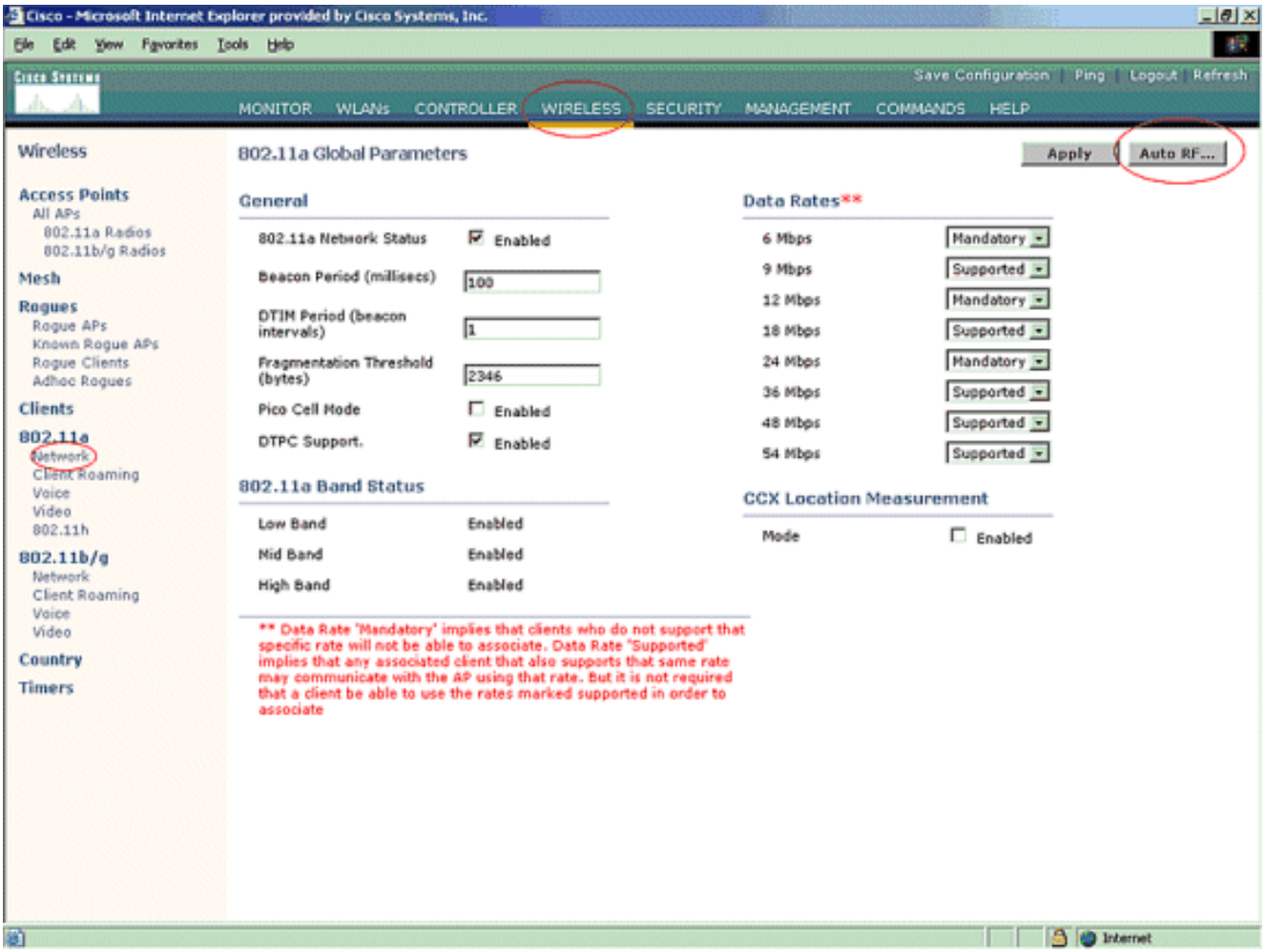
1. Stellen Sie sicher, dass das Protokoll für die Erkennung nicht autorisierter Standorte aktiviert ist. Um sie zu aktivieren, wählen Sie **Security > Rogue Policies (Sicherheit > Nicht autorisierte Richtlinien) aus,** und klicken Sie wie in der Abbildung gezeigt im **Rogue Location Discovery Protocol** auf **Enabled (Aktiviert)**.**Hinweis:** Wenn ein nicht autorisierter Access Point eine bestimmte Zeit lang nicht hörbar ist, wird er vom Controller entfernt. Dies ist das **Ablaufzeitlimit** für einen nicht autorisierten Access Point, das unter der RLDP-Option konfiguriert
wird.



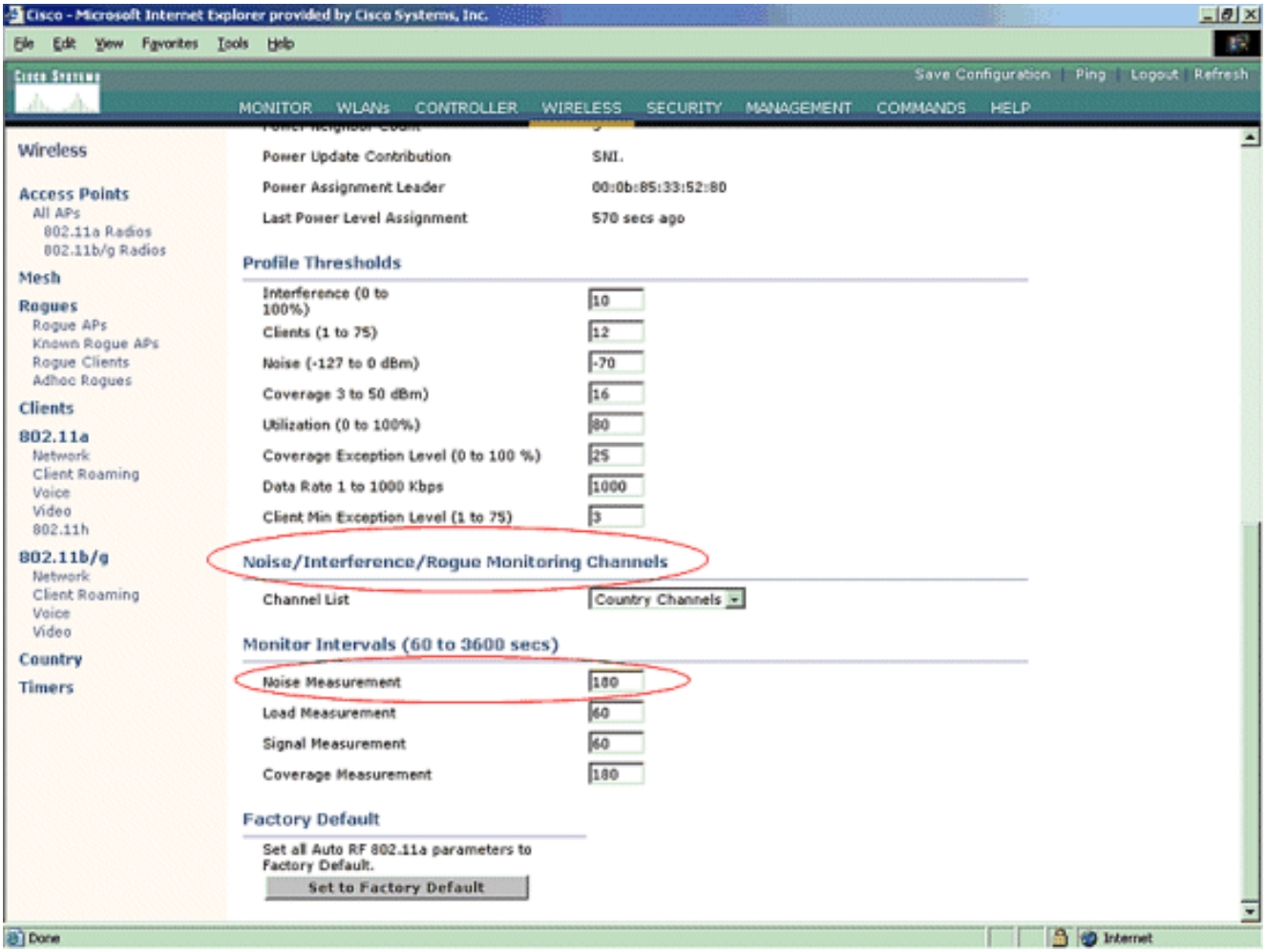
2. Dies ist ein optionaler Schritt. Wenn diese Funktion aktiviert ist, werden die APs, die RRM-Nachbarpakete mit unterschiedlichen **RF-Gruppen-**Namen senden, als unberechtigte Pakete gemeldet. Dies ist hilfreich bei der Untersuchung Ihrer Funkumgebung. Wählen Sie zur Aktivierung die Option **Security-> AP Authentication (Sicherheit > AP-Authentifizierung)**. Wählen Sie dann **AP Authentication** als Schutztyp aus, wie in der Abbildung dargestellt.



3. Überprüfen Sie die zu scannenden Kanäle in den folgenden Schritten:Wählen Sie **Wireless > 802.11a Network aus**, und **Auto RF**, wie in der Abbildung gezeigt, rechts.



Blättern Sie auf der Seite **Auto RF** nach unten, und wählen Sie **Noise/Interference/Rogue Monitoring Channels aus**.



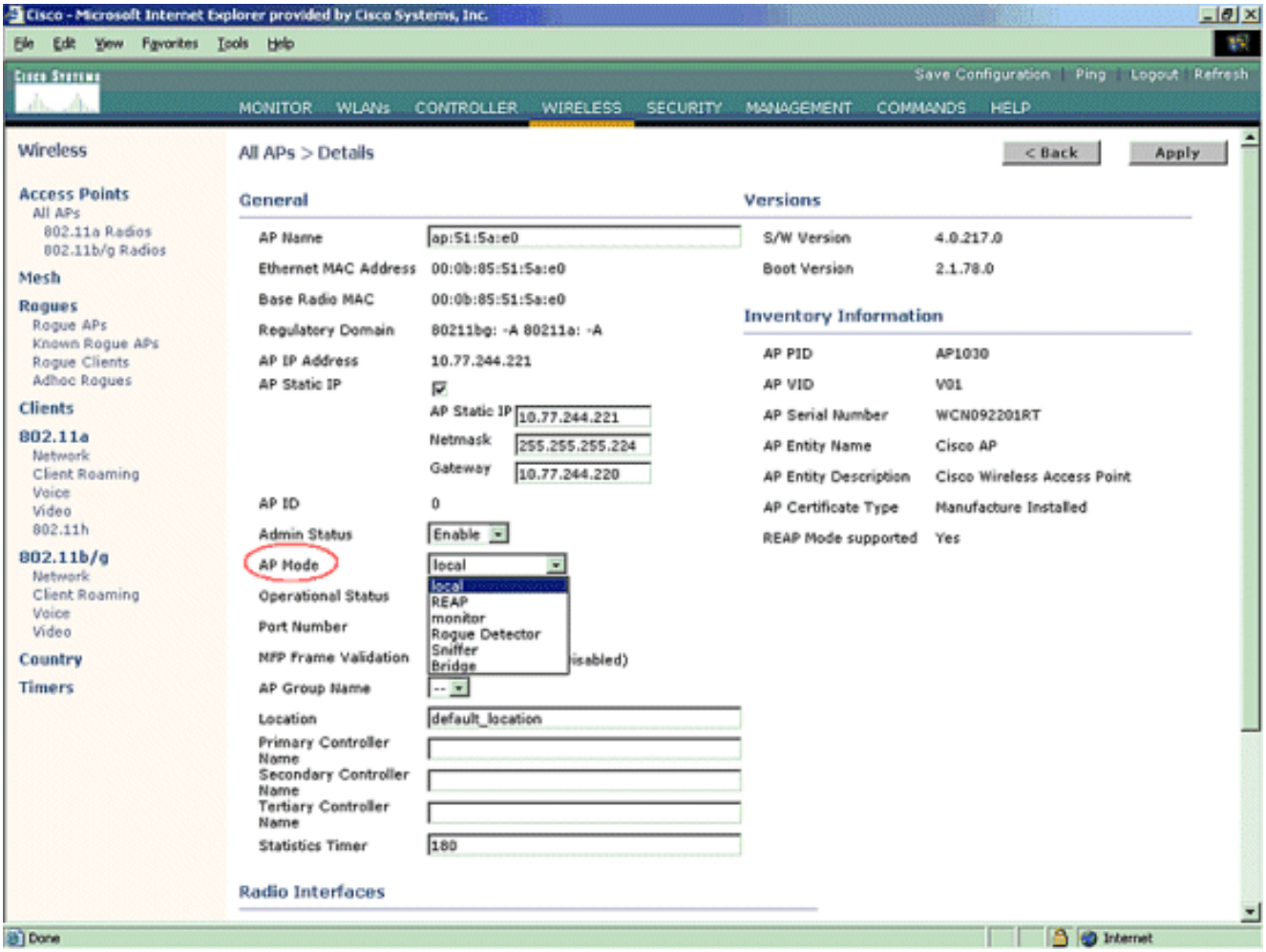
In der Kanalliste werden neben anderen Controller- und AP-Funktionen auch die Kanäle aufgeführt, die auf die Überwachung von nicht autorisierten Geräten gescannt werden sollen. Weitere Informationen zu einfachen APs und Wireless LAN Controller (WLC) Troubleshoot FAQ finden Sie in den Lightweight Access Point FAQ (Häufig gestellte Fragen zu Wireless-Controllern).

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Zeitraum für das Scannen ausgewählter Kanäle festlegen:Die Abtastdauer der definierten Kanalgruppe wird unter **Überwachungsintervall > Rauschmessung** konfiguriert, und der zulässige Bereich liegt zwischen 60 und 3600 Sekunden. Wenn die Standardeinstellung von 180 Sekunden beibehalten wird, scannen die APs jeden Kanal in der Kanalgruppe einmal 50 ms alle 180 Sekunden. Während dieses Zeitraums wechselt das AP-Funkmodul von seinem Dienstkanal zum angegebenen Kanal, überwacht und zeichnet Werte für einen Zeitraum von 50 ms auf und kehrt dann zum ursprünglichen Kanal zurück. Die Hop-Zeit plus die Verweilzeit von 50 ms nimmt den Access Point für ca. 60 ms jedes Mal außer Kanal. Das bedeutet, dass jeder Access Point ungefähr 840 ms von den insgesamt 180 Sekunden damit

verbringt, auf unberechtigte Personen zu hören.Die "Listen"- oder "Verweilzeit"-Zeit kann nicht geändert werden und wird durch eine Anpassung des Rauschmesswerts nicht geändert. Wenn der Timer für die Geräuschmessung gesenkt wird, werden im unberechtigten Erkennungsprozess wahrscheinlich weitere unberechtigte Treffer gefunden und diese schneller gefunden. Diese Verbesserung geht jedoch zulasten der Datenintegrität und des Kundenservice. Ein höherer Wert dagegen ermöglicht eine bessere Datenintegrität, verringert jedoch die Fähigkeit, unberechtigte Personen schnell zu finden.

5. Konfigurieren Sie den AP-Betriebsmodus:Ein einfacher AP-Betriebsmodus definiert die Rolle des AP. Folgende Modi beziehen sich auf die in diesem Dokument vorgestellten Informationen:**Local (Lokal**) - Dies ist der normale Betrieb eines Access Points. Dieser Modus ermöglicht die Wartung von Daten-Clients, während konfigurierte Kanäle auf Geräusche und Schurken gescannt werden. In diesem Betriebsmodus verliert der Access Point 50 ms den Kanal und hört auf Schurken. Er durchläuft jeden Kanal einzeln und für den in der Auto RF-Konfiguration angegebenen Zeitraum.**Monitor** - Dies ist der Modus "Radio Receive Only" (Nur Funkempfang), mit dem der Access Point alle 12 Sekunden alle konfigurierten Kanäle scannen kann. Nur Entauthentifizierungspakete werden in der Luft gesendet, wobei ein AP so konfiguriert ist. Ein Überwachungsmodus-AP kann unberechtigte Geräte erkennen, kann jedoch keine Verbindung zu einem verdächtigen, unberechtigten Benutzer als Client herstellen, um die RLDP-Pakete zu senden.**Hinweis:** DCA bezieht sich auf nicht überlappende Kanäle, die mit den Standardmodi konfiguriert werden können.**Rogue Detector** (**Rogue Detector**): In diesem Modus ist der AP-Sender ausgeschaltet, und der Access Point überwacht nur den kabelgebundenen Datenverkehr. Der Controller übergibt die APs, die als nicht autorisierte Detektoren konfiguriert sind, sowie Listen verdächtiger nicht autorisierter Clients und AP-MAC-Adressen. Der nicht autorisierte Detektor hört nur ARP-Pakete ab und kann bei Bedarf über eine Trunk-Verbindung mit allen Broadcast-Domänen verbunden werden.Sie können einfach einen einzelnen AP-Modus konfigurieren, sobald der Lightweight AP mit dem Controller verbunden ist. Um den AP-Modus zu ändern, stellen Sie eine Verbindung zur Webschnittstelle des Controllers her, und navigieren Sie zu **Wireless**. Klicken Sie auf **Details** neben dem gewünschten Access Point, um einen Bildschirm anzuzeigen, der diesem
ähnelt:



Wählen Sie im Dropdown-Menü AP Mode (AP-Modus) den gewünschten AP-Betriebsmodus aus.

Befehle zur Fehlerbehebung

Sie können diese Befehle auch verwenden, um eine Fehlerbehebung für Ihre Konfiguration auf dem Access Point durchzuführen:

- **show rogue ap summary** - Dieser Befehl zeigt die Liste der nicht autorisierten Access Points an, die von den Lightweight APs erkannt wurden.
- **show ungue ap detail** ***<MAC-Adresse der unberechtigten ap>*** **-** Verwenden Sie diesen Befehl, um Details zu einem einzelnen nicht autorisierten Access Point anzuzeigen. Mit diesem Befehl kann festgestellt werden, ob der nicht autorisierte Access Point an das kabelgebundene Netzwerk angeschlossen ist.

Schlussfolgerung

Die Erkennung und Eindämmung von nicht autorisierten Zugriffen innerhalb der zentralen Cisco Controller-Lösung ist die effektivste und am wenigsten störende Methode der Branche. Dank der Flexibilität, die Netzwerkadministratoren erhalten, können sie individuelle Lösungen bereitstellen, die alle Netzwerkanforderungen erfüllen.

Zugehörige Informationen

- Überblick über RF-Gruppen
- Technischer Support und Dokumentation - Cisco Systems