Ruggendetectie onder Unified draadloze netwerken

Inhoud

Inleiding

Draadloze netwerken breiden bekabelde netwerken uit en verhogen de productiviteit van de werknemers en de toegang tot informatie. Een niet-geautoriseerd draadloos netwerk vormt echter een extra laag beveiligingsproblemen. Minder gedachte wordt in havenveiligheid op bedrade netwerken gebracht, en draadloze netwerken zijn een makkelijke uitbreiding tot bekabelde netwerken. Daarom kan een medewerker die zijn of haar eigen Cisco Access Point (AP) in een goed beveiligde draadloze of bekabelde infrastructuur brengt en onbevoegde gebruikers toegang tot dit anders beveiligde netwerk toestaan, een beveiligd netwerk makkelijk in gevaar brengen.

De detectie van de schurk staat de netwerkbeheerder toe om dit veiligheidsprobleem te controleren en te elimineren. Cisco Unified Network Architecture biedt twee methoden voor detectie van schurken die een volledige oplossing voor identificatie en insluiting mogelijk maken zonder dat u dure en moeilijk te rechtvaardigen overlay netwerken en tools nodig hebt.

Overzicht van functies

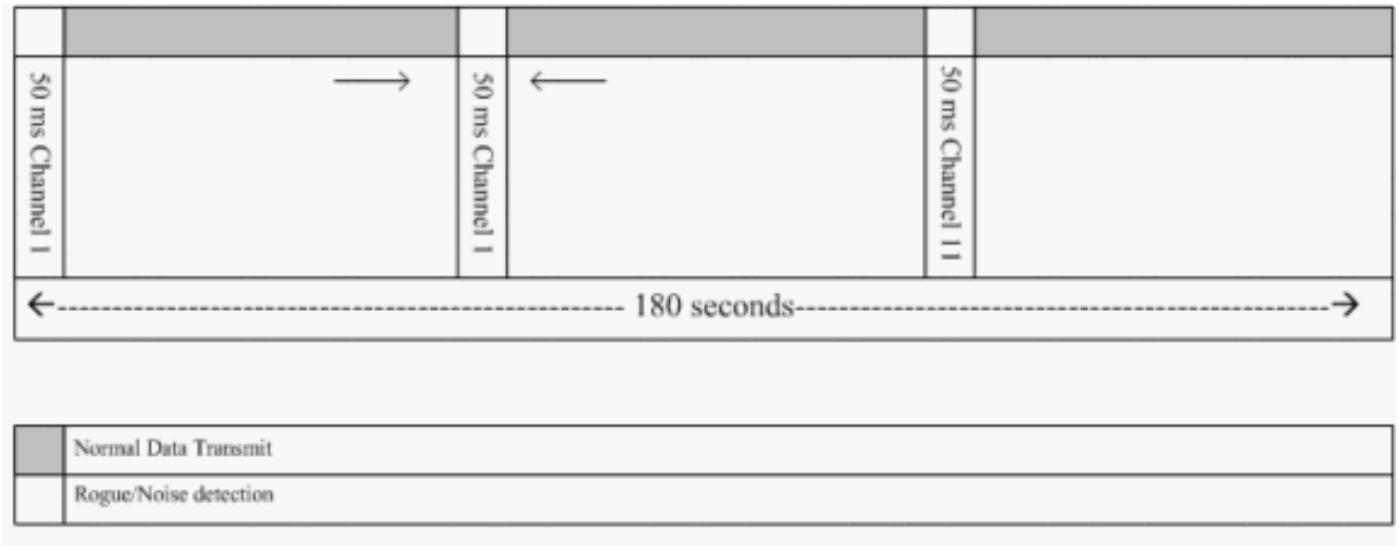
De detectie van schurken is niet gebonden aan enige regelgeving en voor de werking ervan is geen wettelijke naleving vereist. Een dergelijke beperking brengt echter meestal juridische problemen met zich mee die de infrastructuuraanbieders in een ongemakkelijke positie kunnen brengen als zij automatisch moeten opereren. Cisco is extreem gevoelig voor dergelijke problemen en biedt deze oplossingen. Elke controller is ingesteld met een RF Group name.Zodra een lichtgewicht AP zich registreert bij een controller, wordt er een **verificatie-informatie-element (IE)** ingebouwd dat specifiek is voor de RF-groep die op de controller is ingesteld in al zijn beacons/probe-responsframes. Wanneer de lichtgewicht AP beacons/sonde antwoordkaders van AP van AP zonder deze **IE** of met **verkeerde IE** hoort, dan meldt Lichtgewicht AP dat AP als schurk, zijn BSSID in een schurkentafel registreert en de tabel naar de controller stuurt. Er zijn

twee methoden, namelijk het Protocol inzake de ontdekking van schurkenlocatie (RLDP) en de passieve exploitatie, die uitvoerig worden toegelicht; Zie het gedeelte Actieve Rogen bepalen.

Detectie van infrastructuurvoorzieningen

Ruwe ontdekkingen in een actieve draadloze omgeving kunnen kostbaar zijn. Dit proces vraagt AP in dienst (of lokale modus) om de dienst te beëindigen, op lawaai te luisteren en schurkendetectie uit te voeren. De netwerkbeheerder vormt de te scannen kanalen en vormt de tijdspanne waarin alle stations worden gescand. AP luistert naar 50 ms voor heftige clientbundels en dan naar het geconfigureerde kanaal om klanten opnieuw te bedienen. Dit actieve scannen, gecombineerd met buurberichten, identificeert welke AP's rogen zijn en welke AP's geldig zijn en deel uitmaken van het netwerk. Om de gescande kanalen en de scantijd te configureren bladert u naar **Draadloos > 802.11b/g Netwerk** (**b/g** of "**a**" afhankelijk van de netwerkvereisten) en selecteert u de **Auto RF**-knop in de rechterbovenhoek van het browser venster.

U kunt naar **kanalen voor alarmbewaking/interferentie-/schurkenbewaking** scannen om de te scannen kanalen voor ruis en ruis te configureren. De beschikbare opties zijn: Alle kanalen (1 tot en met 14), landkanalen (1 tot en met 11) of Dynamic Channel Association (DCA) kanalen (standaard 1, 6 en 11). De scantijd via deze kanalen kan in hetzelfde venster worden ingesteld, **naast** het interval voor het meten van ruis onder **Monitor Intervallen (60 tot 3600 seconden)**. Standaard is het luisterinterval voor off-channel ruis 180 seconden. Dit betekent dat elk kanaal elke 180 seconden wordt gescand. Dit is een voorbeeld van de kanalen DCA die om de 180 seconden worden gescand:



Zoals wordt geïllustreerd, laat een groot aantal kanalen die worden gescand in combinatie met de korte scanintervallen, minder tijd voor AP om daadwerkelijk gegevensklanten te bedienen.

De lichtgewicht AP wacht om klanten en AP's als rogen te etiketteren omdat deze rogen mogelijk niet door een andere AP worden gemeld totdat een andere cyclus is voltooid. Dezelfde AP beweegt opnieuw naar hetzelfde kanaal om op schurkenaccess points en clients te controleren, zowel als ruis en interferentie. Indien dezelfde klanten en/of AP's worden gedetecteerd, worden zij opnieuw in de lijst opgenomen als rogues op de controller. De controller bepaalt nu of deze groepen op het lokale netwerk zijn aangesloten of op een naburige AP. In beide gevallen wordt AP die geen deel uitmaakt van het beheerde lokale draadloze netwerk als schurk beschouwd.

Spraaldetails

Een lichtgewicht AP gaat van kanaal weg voor 50 ms om voor schurkencliënten, monitor voor lawaai, en kanaalverstoring te luisteren. Alle gedetecteerde frauduleuze klanten of AP's worden naar de controller gestuurd, die deze informatie verzamelt:

- Het analoge AP MAC-adres
- De naam van de frauduleuze AP
- Het MAC-adres van de sterk verbonden client(en)
- Of de frames beveiligd zijn met WAP of EFN
- De preambule
- De verhouding Signal-to-Noise (SNR)
- Het indicatielampje voor de signaalsterkte van de ontvanger (RSSI)

Ruggendetector access point

U kunt een AP als schurkendetector laten functioneren, wat het toelaat om op een boomstampoort te worden geplaatst zodat het alle verbonden VLAN's kan horen. Het gaat om het vinden van de client op het bekabelde netwerk op alle VLAN's. De schurkendetector AP luistert naar de pakketten Adreventie Protocol (ARP) om de Layer 2 adressen van geïdentificeerde schurkencliënten of schurkenAP's te bepalen die door de controller worden verzonden. Als een Layer 2-adres dat bij elkaar komt, genereert de controller een alarm dat de frauduleuze AP of client als een bedreiging identificeert. Dit alarm geeft aan dat de schurk gezien werd op het bekabelde netwerk.

Active Rogues bepalen

Roepachtige AP's moeten twee keer worden "gezien" voordat ze door de controller als schurk worden toegevoegd. Rogue AP's worden niet als een bedreiging beschouwd als ze niet zijn verbonden met het brede segment van het bedrijfsnetwerk. Om te bepalen of de schurk actief is, worden verschillende benaderingen gebruikt. Een van die benaderingen is RLDP.

Real-Location Discovery Protocol (RLDP)

RLDP is een actieve benadering, die wordt gebruikt wanneer frauduleuze AP geen verificatie (Open Verificatie) heeft ingesteld. Deze modus, die standaard uitgeschakeld is, geeft een actieve AP op om naar het schurkenkanaal te gaan en verbinding te maken met de regelaar als client. Gedurende deze tijd verstuurt de actieve AP alle aangesloten klanten deauthenticatieberichten en sluit dan de radio interface. Dan associeert het met de schurkenpas als cliënt.

AP probeert dan een IP adres van schurft AP te verkrijgen en verstuurt een pakket van het Protocol van de Gebruiker Datagram (UDP) (poort 6352) dat de lokale AP en de verbindingsinformatie aan de controller door schurkenAP bevat. Als de controller dit pakket ontvangt, wordt het alarm ingesteld om de netwerkbeheerder ervan op de hoogte te stellen dat er een frauduleus AP is ontdekt op het bekabelde netwerk met de RLDP-functie.

Opmerking: Gebruik het **debug dot11 rldp om** opdracht in te schakelen om te controleren of de lichtgewicht AP een DHCP-adres van de schurkenzone associeert en ontvangt. Deze opdracht geeft ook het UDP-pakket weer dat door de lichtgewicht AP naar de controller is verzonden.

Er wordt hier een voorbeeld weergegeven van een UDP-pakket (bestemmingpoort 6352) dat door lichtgewicht AP wordt verzonden:

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

De eerste 5 bytes van de gegevens bevatten het DHCP-adres dat aan de lokale mode AP door de schurkenzone wordt gegeven. De volgende 5 bytes zijn het IP-adres van de controller, gevolgd door 6 bytes die het frauduleuze AP MAC-adres weergeven. Dan zijn er 18 bytes van nul.

passieve bediening:

Deze benadering wordt gebruikt wanneer frauduleuze AP een of andere vorm van authenticatie heeft, of de anti-mode-aanval of de anti-vorm-koppelteken van de computer. Wanneer een vorm van authenticatie is ingesteld op frauduleuze AP, kan de Lichtgewicht AP niet associëren omdat het de sleutel niet kent die op de schurkenAP wordt gevormd. Het proces begint met de controller wanneer deze op de lijst van schurkenclient-MAC-adressen wordt doorgegeven aan een AP dat is ingesteld als schurkendetector. De schurkendetector scant alle aangesloten en gevormde subnetten voor ARP verzoeken, en ARP zoekopdrachten naar een overeenkomend Layer 2 adres. Als een overeenkomst wordt ontdekt, meldt de controller de netwerkbeheerder dat een regelaar wordt gedetecteerd op het bedrade net.

Active Rogue-beheersing

Zodra een frauduleuze client wordt gedetecteerd op het bekabelde netwerk, kan de netwerkbeheerder zowel de schurft AP als de schurkencliënten bevatten. Dit kan worden bereikt omdat de pakketten 802.11 van de authenticatie naar klanten worden verzonden die aan schurkenluiders worden geassocieerd zodat de dreiging die een dergelijk gat veroorzaakt wordt verminderd. Elke keer dat er een poging is om frauduleus AP in te dammen wordt bijna 15% van het lichtgewicht AP's middelen gebruikt. Daarom wordt geadviseerd om de schurkenzone fysiek te plaatsen en te verwijderen zodra deze is ingesloten.

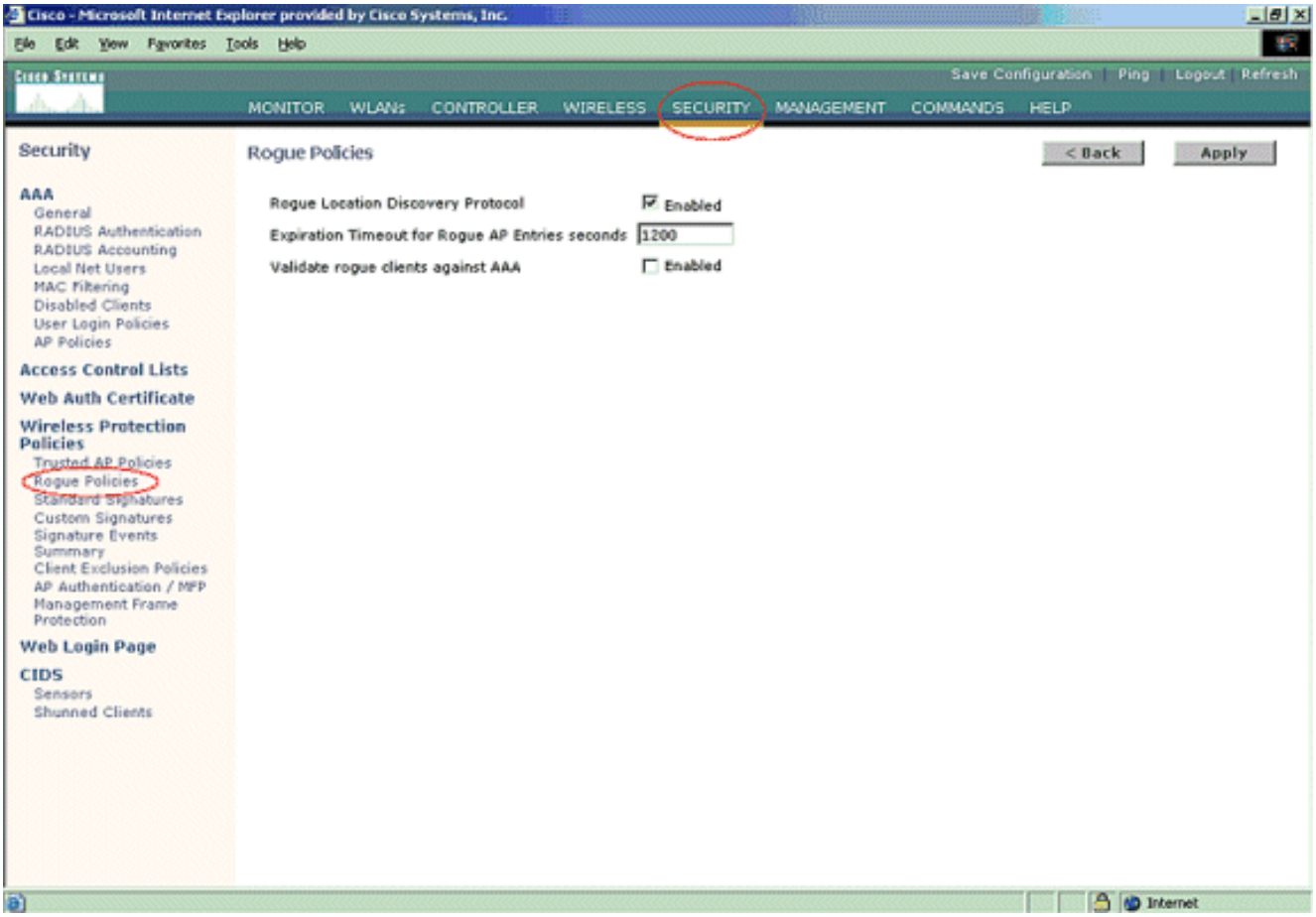
OPMERKING: Vanaf de WLC release 5.2.15.0 kunt u er nu voor kiezen om de gedetecteerde ruis handmatig of automatisch in te sluiten. In besturingssoftwarereleases voorafgaand aan 5.2.157.0 is handmatige insluiting de enige optie.

Detectie tijdens rotaties - Configuratiescherm

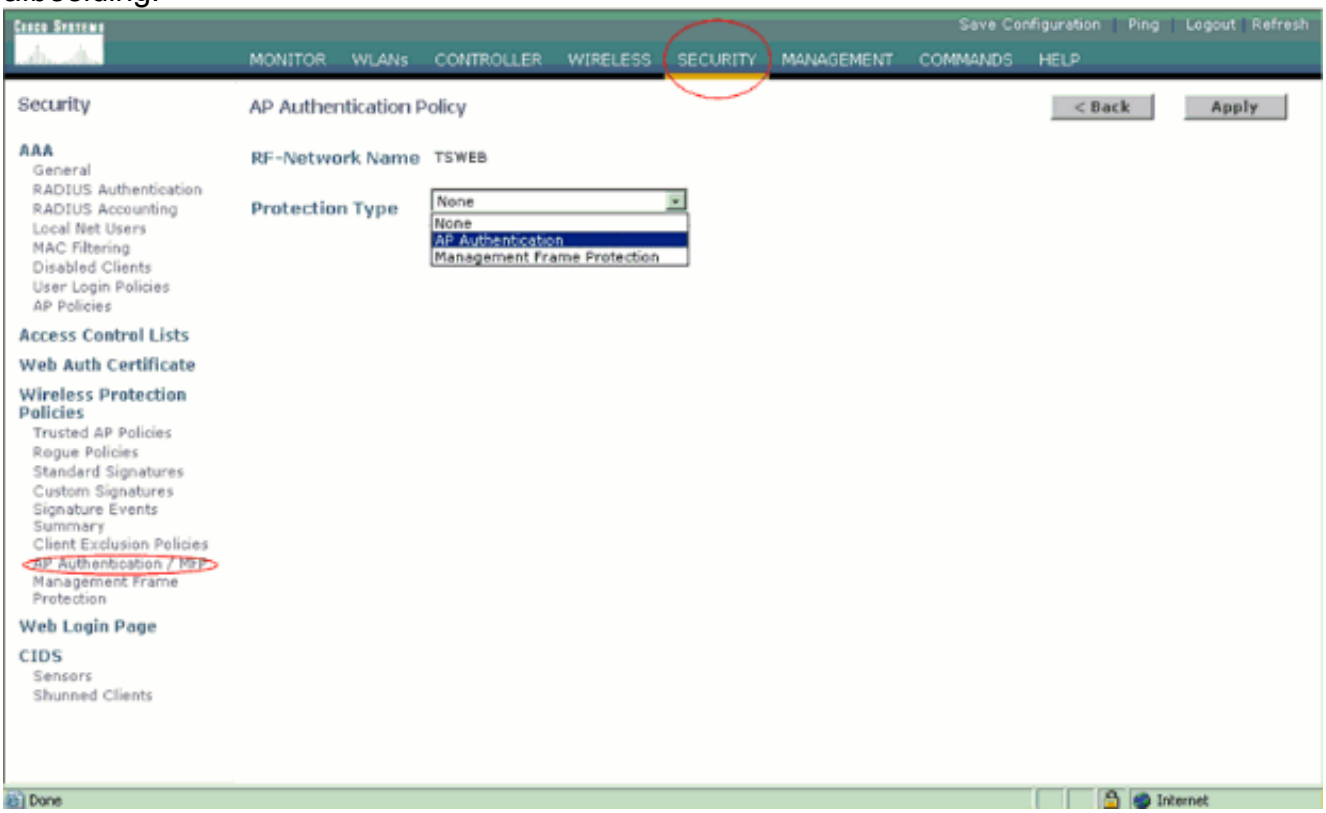
Bijna de gehele configuratie van de schurkendetectie is standaard ingeschakeld om maximale, out-of-the-box netwerkbeveiliging mogelijk te maken. Bij deze configuratiestappen wordt ervan uitgegaan dat er geen frauduleuze detectie op de controller is ingesteld om belangrijke schurkendetectie-informatie te verduidelijken.

Voltooi de volgende stappen om een detectie van een storing in te stellen:

1. Zorg ervoor dat het protocol voor de detectie van de locatie van Rogue is ingeschakeld. Om het programma in te schakelen, kiest u **Beveiligings- > Tandenbeleid** en klikt u op **Ingeschakeld** op **Verkenningsprotocol** bij de **lokatie** zoals in de afbeelding.**Opmerking:** Als een frauduleus AP gedurende een bepaalde tijd niet wordt gehoord, wordt het uit de controller verwijderd. Dit is de **Time-out voor** beëindiging van het **programma** voor schurft AP, dat is ingesteld onder de RLDP-
optie.

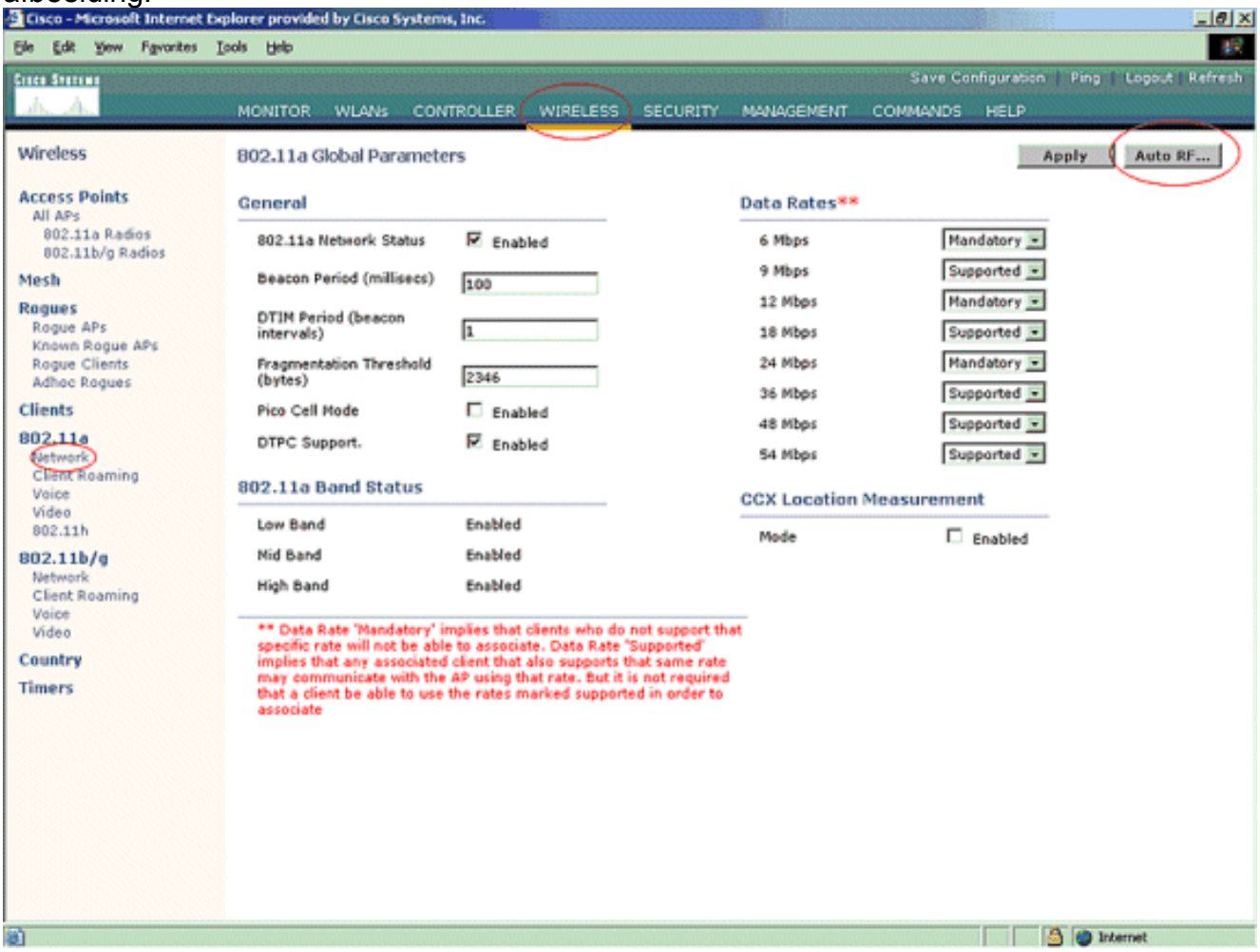


2. Dit is een optionele stap. Als deze optie is ingeschakeld, worden AP's die RRM buurpakketten met verschillende **RF Group** namen verzenden als rogues gerapporteerd. Dit zal helpen bij het bestuderen van uw RF-omgeving. Kies **Security-> AP-verificatie** om deze **in** te schakelen. Kies vervolgens **AP-verificatie** als het beschermingstype zoals in de afbeelding.

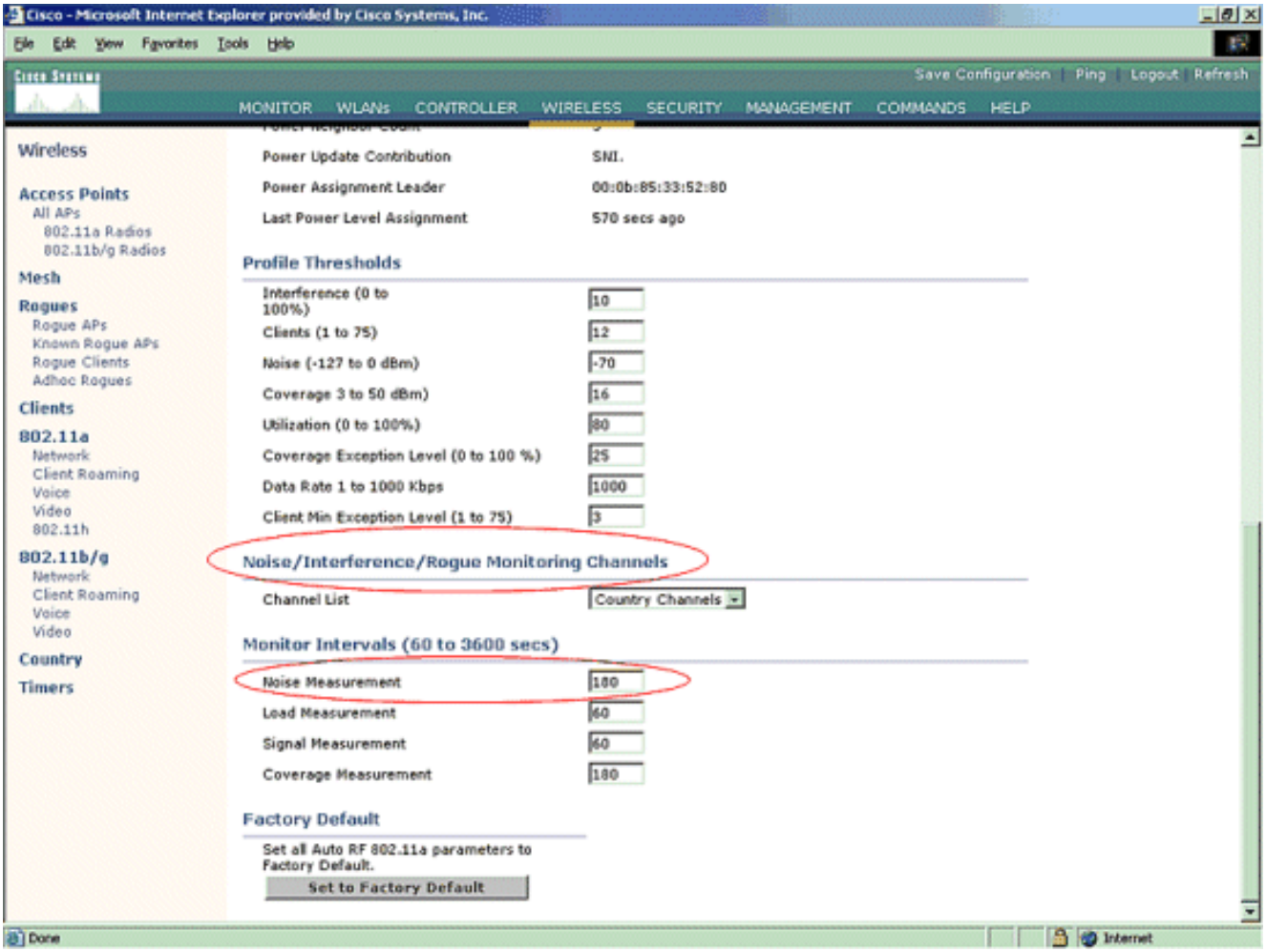


3. Controleer de kanalen die in deze stappen moeten worden gescand:Selecteer **Draadloos > 802.11a-netwerk** en **Auto RF** aan de rechterkant zoals in de

afbeelding.



Op de **Auto RF**-pagina scrollen en kiezen **u** de **kanalen voor bewaking van ruis/interferentie/scheuren**.



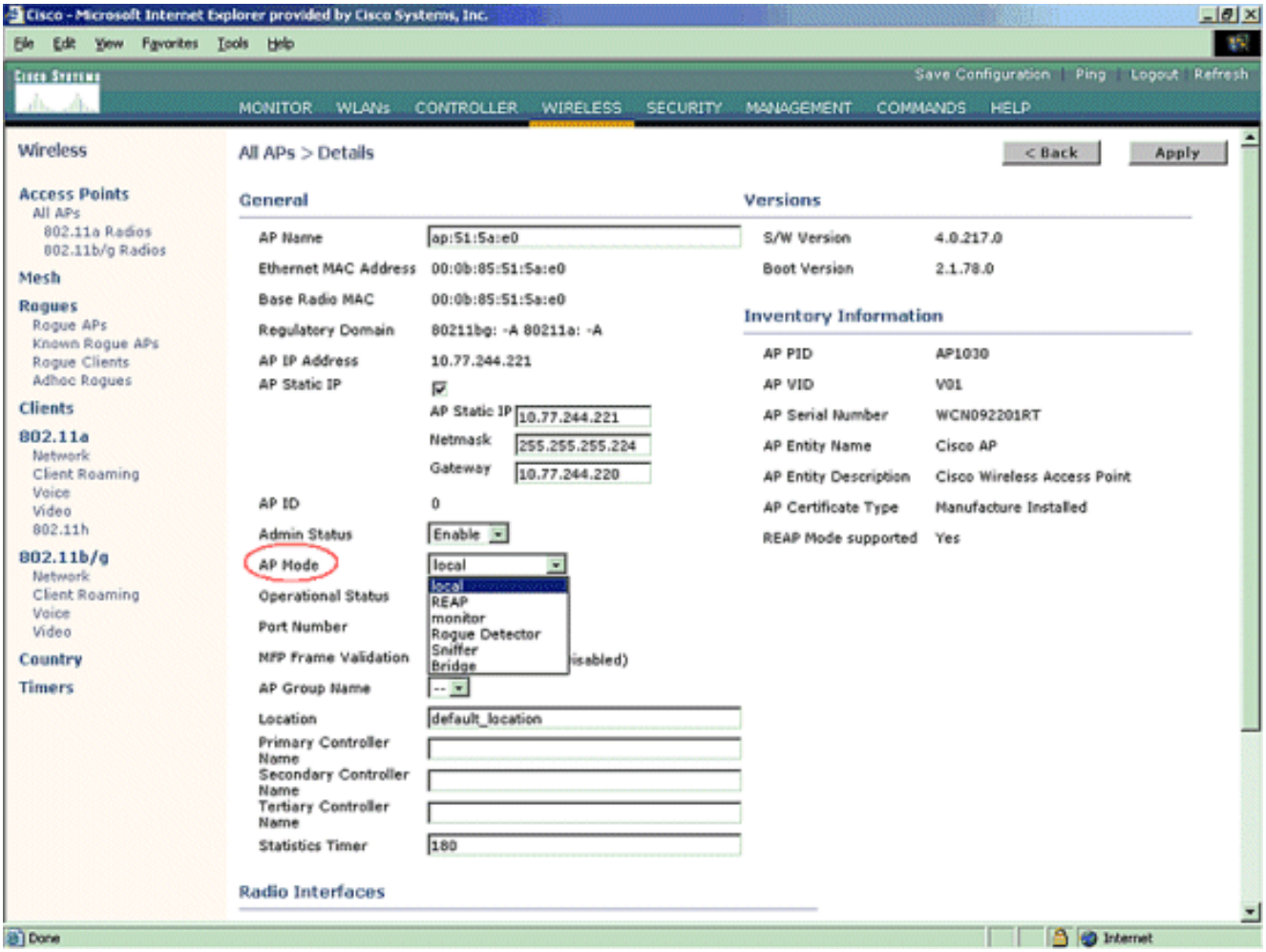
In de Kanaallijst worden de kanalen die voor alarmbewaking moeten worden gescand, naast andere controller en AP-functies, gespecificeerd. Raadpleeg het gedeelte [Lichtgewicht access point FAQ](#) voor meer informatie over lichtgewicht AP's en [draadloze LAN Controller (WLC) probleemoplossing FAQ](#) voor meer informatie over draadloze controllers.

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. Stel de tijdsperiode in voor het scannen van geselecteerde kanalen:De scanduur van de gedefinieerde groep kanalen wordt ingesteld onder **Monitor Intervalen > Geluidsmeting** en het toegestane bereik loopt van 60 tot 3600 seconden. Als dit item wordt ingesteld op 180 seconden, scannen de AP's elk kanaal eenmaal in de kanaalgroep, 50 ms, elke 180 seconden. Gedurende deze periode verandert de AP-radio van zijn servicekanaal naar het gespecificeerde kanaal, luistert en registreert waarden voor een periode van 50 ms, en keert dan terug naar het oorspronkelijke kanaal. De hoptijd plus de dwell tijd van 50 ms neemt AP van kanaal af voor ongeveer 60 ms elke keer. Dit betekent dat elke AP ongeveer 840 ms van de totale 180 seconden besteedt aan het luisteren naar een tasje.De "luister"- of "dwell"-tijd

kan niet worden gewijzigd en wordt niet gewijzigd met een aanpassing van de waarde van de geluidsmeting. Als de timer voor de geluidsmeting is verlaagd, zal het schurkenonderzoek waarschijnlijk meer rogen vinden en ze sneller vinden. Deze verbetering gaat echter ten koste van de gegevensintegriteit en de dienstverlening aan de cliënt. Een hogere waarde daarentegen maakt een betere gegevensintegriteit mogelijk, maar vermindert het vermogen om snel rogen te vinden.

5. Configuratie van de AP wijze van bediening:De rol van het AP wordt gedefinieerd door een lichtgewicht AP-modus. De modi met betrekking tot de informatie in dit document zijn:**Lokaal**: dit is de normale werking van een AP. In deze modus kan gegevensclients worden onderhouden terwijl de geconfigureerde kanalen gescand zijn voor ruis en rogen. In deze manier van functioneren, gaat AP over 50 ms van het kanaal en luistert naar rogen. Het programma loopt door elk kanaal, één voor één, voor de periode die bij de Auto RF-configuratie is gespecificeerd.**Monitor** - Dit is radio ontvangt slechts modus, en laat AP toe om alle geconfigureerde kanalen elke 12 seconden te scannen. Alleen de-authenticatie-pakketten worden in de lucht verzonden met een AP die zo wordt geconfigureerd. Een AP in de monitor modus kan rogen detecteren, maar het kan geen verbinding maken met een verdachte rok als client om de RLDP-pakketten te verzenden.**Opmerking:** DCA verwijst naar niet-overlappende kanalen die compatibel zijn met de standaardmodi.**Rugudetectie** - In deze modus, wordt de AP-radio uitgeschakeld en luistert de AP naar alleen bekabeld verkeer. De controller geeft de AP's die zijn ingesteld als schurkendetectoren, alsook lijsten van verdachte klanten en AP MAC-adressen, door. De schurkendetector luistert alleen naar ARP-pakketten en kan indien gewenst met alle uitzending-domeinen door een hoofdlink worden verbonden.U kunt een individuele AP-modus eenvoudig configureren, zodra de lichtgewicht AP is aangesloten op de controller. Om de AP-modus te wijzigen, sluit u aan op de controller web-interface en navigeer naar **Wireless**. Klik op **Details** naast de gewenste AP to om een scherm weer te geven dat vergelijkbaar is met
dit:



Gebruik het vervolgkeuzemenu AP-modus om de gewenste AP-modus te selecteren.

Opdrachten voor troubleshooting

U kunt deze opdrachten ook gebruiken om problemen met uw configuratie op het AP op te lossen:

- **toon overzicht van** het **scheervenster**-Deze opdracht toont de lijst van schurkenaccess points die door lichtgewicht APs worden gedetecteerd.
- **Toon gedetailleerde *<MAC-adres van de schurkenkap>*-**Gebruik deze opdracht om gegevens over een afzonderlijke schurft-AP weer te geven. Dit is de opdracht die helpt vast te stellen of de schurft-AP op het bekabelde netwerk is aangesloten.

Conclusie

De detectie en insluiting van schurken binnen de gecentraliseerde controller van Cisco is de meest effectieve en minst opdringerige methode in de sector. De aan de netwerkbeheerder geboden flexibiliteit maakt een meer aangepaste pasvorm mogelijk die kan voorzien in netwerkvereisten.

Gerelateerde informatie

- Overzicht van RF-groepen
- Technische ondersteuning en documentatie – Cisco Systems