

Schaduwdetectie en -beperking oplossen in een Unified Wireless Network

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Schurkenoverzicht](#)

[Schurkendetectie](#)

[Off-Channel scan](#)

[Monitormodus scannen](#)

[Vergelijking van lokale modus en monitormodus](#)

[Identificatie van fraude](#)

[Rogue Records](#)

[Rogue Details](#)

[Rogue-gebeurtenissen exporteren](#)

[Time-out bij Rogue Record](#)

[Schurfdetectie - AP](#)

[schaalbaarheidsoverwegingen](#)

[RLDP](#)

[Voorbehouden bij RLDP](#)

[Switch-poortsporen](#)

[Schurkenclassificatie](#)

[Schurkenclassificatieregels](#)

[HA Feiten](#)

[Flex-Connect - feiten](#)

[Kreukvrij](#)

[Schurkenbeperking](#)

[Details van Rogue Containment](#)

[Automatische insluiting](#)

[Voorbehouden bedriegers](#)

[Switch Port Shut](#)

[Configureren](#)

[Schurfdetectie configureren](#)

[Kanaalscan configureren voor detectie van fouten](#)

[Schurkenclassificatie configureren](#)

[Kreukvrij configureren](#)

[Handmatige insluiting instellen](#)

[Automatische insluiting](#)

[Met Prime-infrastructuur](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Als de schurk niet wordt herkend](#)

[Handige debugs](#)

[Verwachte Trap-logbestanden](#)

[Aanbevelingen](#)

[Als de Rogue niet geclassificeerd is](#)

[Handige debugs](#)

[Aanbevelingen](#)

[RLDP identificeert geen Rogues](#)

[Handige debugs](#)

[Aanbevelingen](#)

[Schurfdetectie - AP](#)

[Handige debug-opdrachten in een AP-console](#)

[Schurkenbeperking](#)

[Verwachte debugs](#)

[Aanbevelingen](#)

[Conclusie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft detectie en beperking van fraude bij Cisco draadloze netwerken.

Draadloze netwerken breiden bekabelde netwerken uit en verhogen de productiviteit van werknemers en de toegang tot informatie. Een niet-geautoriseerd draadloos netwerk levert echter een extra beveiligingsprobleem op. Minder aandacht wordt besteed aan poortbeveiliging op bekabelde netwerken en draadloze netwerken zijn een eenvoudige uitbreiding naar bekabelde netwerken. Daarom kan een werknemer die zijn of haar eigen access point (Cisco of niet-Cisco) in een goed beveiligde draadloze of bekabelde infrastructuur brengt en onbevoegde gebruikers toegang biedt tot dit anderszins beveiligde netwerk, een beveiligd netwerk eenvoudig compromitteren.

Met fraudedetectie kan de netwerkbeheerder deze beveiligingsprobleem bewaken en verwijderen. Cisco Unified Network Architecture biedt methoden voor fraudedetectie die een volledige oplossing voor schurkenidentificatie en -beperking mogelijk maken zonder dat u dure en moeilijk te rechtvaardigen overlay-netwerken en -tools nodig hebt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze LAN-controllers.
- Cisco Prime-infrastructuur.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Unified draadloze LAN-controllen (5520, 8540 en 3504 Series) waarop versie 8.8.120.0 wordt uitgevoerd.
- Wave 2 APs 1832, 1852, 2802 en 3802 reeks.
- Wave 1 APs 3700, 2700 en 1700 reeks.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Schurkenoverzicht

Elk apparaat dat uw spectrum deelt en niet door u wordt beheerd, kan als een schurk worden beschouwd. Een schurk wordt gevaarlijk in deze scenario's:

- Wanneer u deze optie instelt om dezelfde Service Set Identifier (SSID) te gebruiken als uw netwerk (honeypot).
- Wanneer deze wordt gedetecteerd in het bekabelde netwerk.
- Ad hoc-schurken.
- Setup door een buitenstaander, meestal met kwaadaardige bedoeling.

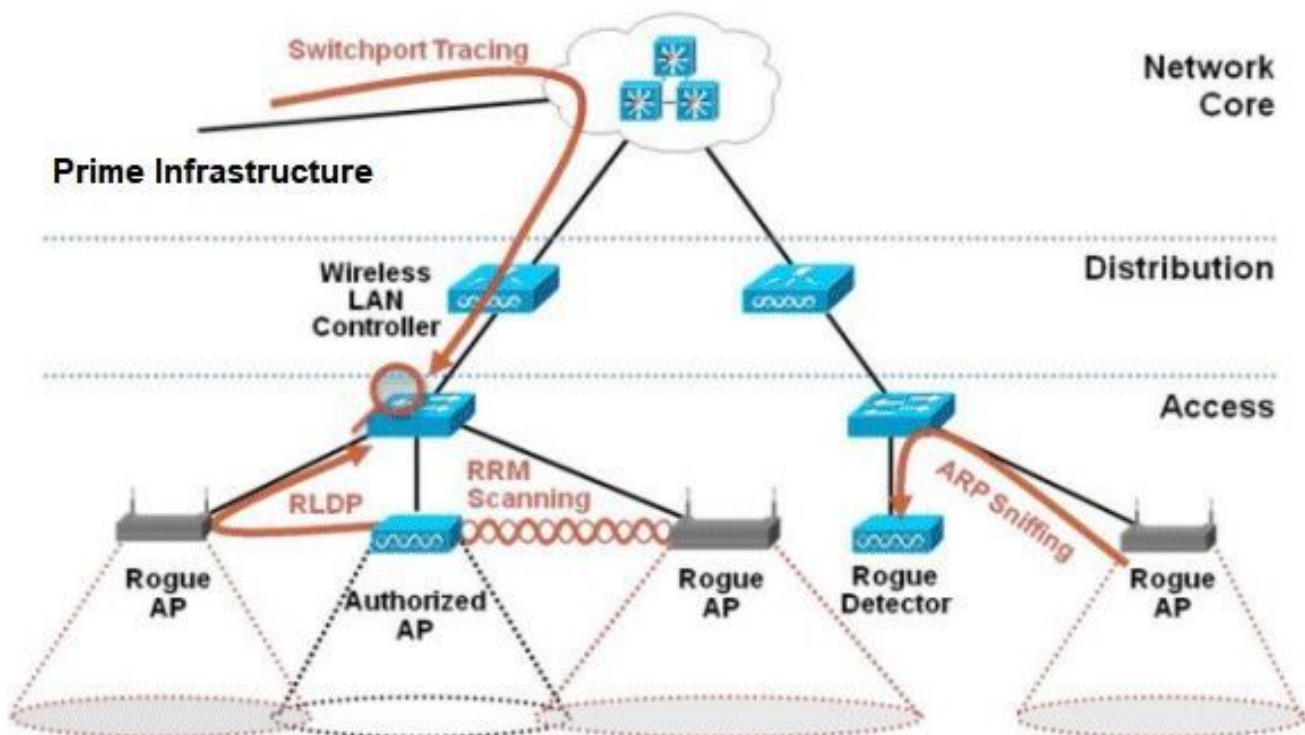
De beste praktijk is schurkendetectie te gebruiken om veiligheidsrisico's te minimaliseren, bijvoorbeeld in een bedrijfsomgeving. Er zijn echter bepaalde scenario's waarin fraudedetectie niet nodig is, bijvoorbeeld bij de implementatie van Office Extend Access Point (OEAP), in de hele stad en buiten. Met het gebruik van outdoor mesh AP's om schurken te detecteren zou weinig waarde bieden terwijl het middelen zou gebruiken om te analyseren. Tot slot is het van cruciaal belang om schurkenautomatische insluiting te evalueren (of helemaal te vermijden), omdat er mogelijke juridische problemen en verplichtingen kunnen ontstaan als deze automatisch worden overgelaten.

Er zijn drie hoofdfasen in bedrieglijk apparaatbeheer in de oplossing Cisco Unified Wireless Network (UWN):

- Detectie - er wordt een Radio Resource Management (RRM)-scan gebruikt om de aanwezigheid van abnormale apparaten te detecteren.
- Classificatie - RLDP (Rogue Location Discovery Protocol), fraudedetectoren (alleen Wave 1 AP's) en sporen van switch-poorten worden gebruikt om te identificeren of het fraudeapparaat is aangesloten op het bekabelde netwerk. Schurkenclassificatieregels helpen ook bij het filteren van schurken in specifieke categorieën op basis van hun kenmerken.
- Mitigation - Switch poort sluiting, schurkenlocatie, en schurkeninsluiting worden gebruikt in om de fysieke locatie op te sporen en de dreiging van het schurkenapparaat ongeldig te maken.

Cisco Rogue Management Diagram

Multiple Methods

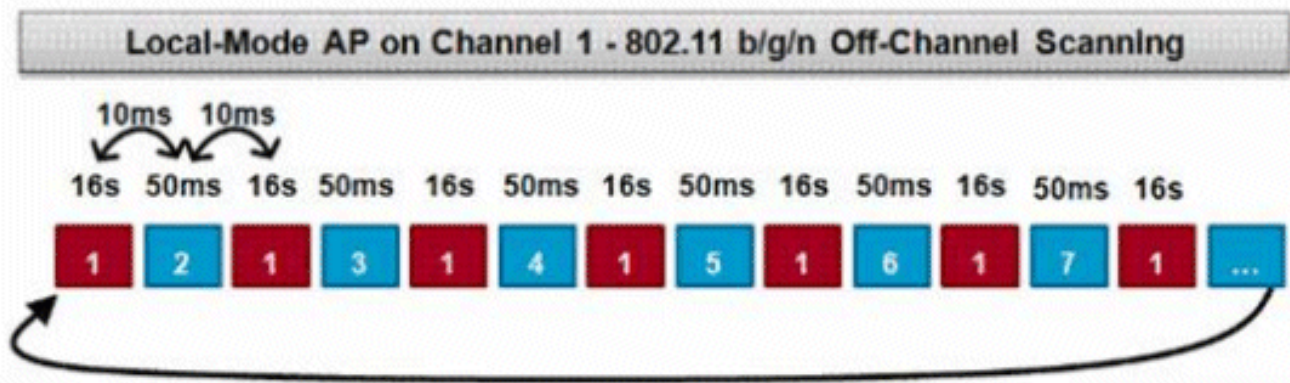


Schurkendetectie

Een schurk is in wezen elk apparaat dat je spectrum deelt, maar niet in je controle is. Dit omvat frauduleuze access points, draadloze router, frauduleuze clients en ad-hocnetwerken. Cisco UWN gebruikt een aantal methoden om Wi-Fi-gebaseerde fraudeapparaten te detecteren, zoals een off-channel scan en speciale monitormodus. Cisco Spectrum Expert kan ook gebruikt worden om schurkenapparaten te identificeren die niet gebaseerd zijn op het 802.11 protocol, zoals Bluetooth-bruggen.

Off-Channel scan

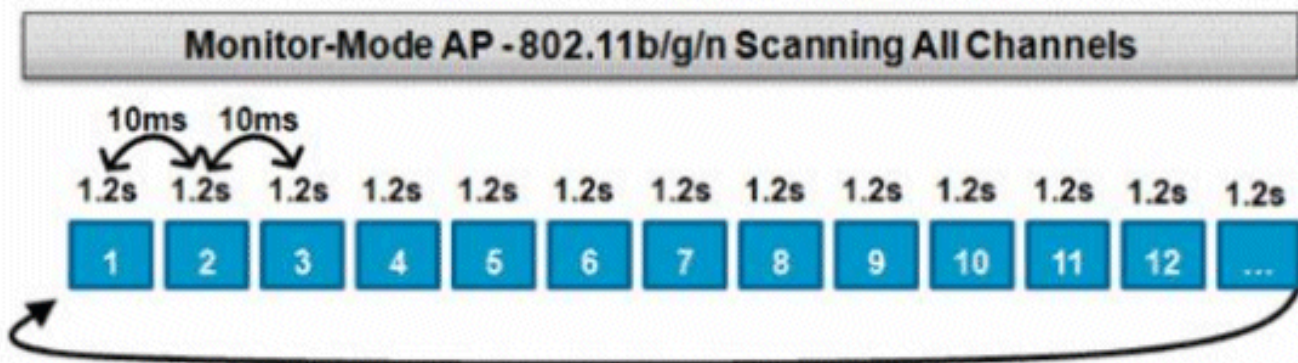
Deze handeling wordt uitgevoerd door lokale toegangspunten en Flex-Connect-toegangspunten (in de verbonden modus) en maakt gebruik van een tijdsegmenteertechniek waarmee clientservices en kanaalscannen met gebruik van dezelfde radio mogelijk zijn. Met de beweging naar off-kanaal voor een periode van 50ms elke 16 seconden, besteedt de AP standaard slechts een klein percentage van zijn tijd om geen klanten te bedienen. Let ook op: er is een 10ms kanaal verandering interval die voorkomen. In de standaard scan interval van 180 seconden, wordt elk 2.4GHz FCC kanaal (1-11) ten minste één keer gescand. Voor andere regelgevingsgebieden, zoals ETSI, is de AP een iets hoger percentage van de tijd uit het kanaal. Zowel de lijst van kanalen als het scaninterval kan worden aangepast in de RRM configuratie. Dit beperkt de impact op de prestaties tot maximaal 1,5% en intelligentie is ingebouwd in het algoritme om de scan op te schorten wanneer QoS-frames met hoge prioriteit, zoals spraak, moeten worden geleverd.



Dit grafisch is een afbeelding van het off-channel scanalgoritme voor een lokale modus AP in de 2.4GHz frequentieband. Een gelijksoortige verrichting wordt gedaan parallel op de radio 5GHz als AP één aanwezig heeft. Elk rood vierkant vertegenwoordigt de tijd die aan het thuiskanaal van de AP's wordt doorgebracht, terwijl elk blauw vierkant de tijd vertegenwoordigt die aan aangrenzende kanalen wordt doorgebracht voor scandoeleinden.

Monitormodus scannen

Deze bewerking wordt uitgevoerd door AP's in de monitormodus en Adaptieve IPS-monitormodus die 100% van de zendtijd gebruiken om alle kanalen in elke respectieve frequentieband te scannen. Hierdoor kan een grotere detectiesnelheid worden bereikt en kan meer tijd worden besteed aan elk afzonderlijk kanaal. De AP's van de monitormodus zijn ook veel superieur bij de detectie van schurkencliënten aangezien zij een uitgebreidere weergave van de activiteit hebben die in elk kanaal voorkomt.



Dit grafisch is een afbeelding van het off-channel scanalgoritme voor een monitormodus AP in de 2.4GHz frequentieband. Een gelijksoortige verrichting wordt gedaan parallel op de radio 5GHz als AP één aanwezig heeft.

Vergelijking van lokale modus en monitormodus

AP van de lokale wijze verdeelt zijn cycli tussen de dienst van de cliënten van WLAN en het aftasten van kanalen voor bedreigingen. Dientengevolge, het duurt lokale wijze AP langer om door alle kanalen te bladeren, en het besteedt minder tijd in de inzamelingsgegevens over om het even welk bepaald kanaal zodat de cliëntverrichtingen niet worden onderbroken. Hierdoor zijn de detectie van schurken en aanvallen langer (3 tot 60 minuten) en kan een kleiner bereik van aanvallen via de lucht worden gedetecteerd dan met een monitor mode AP.

Bovendien is detectie voor bursty verkeer, zoals schurkencliënten, veel minder deterministisch

omdat het toegangspunt op het kanaal van het verkeer moet zijn op het moment dat het verkeer wordt verzonden of ontvangen. Dit wordt een oefening in kansen. Een monitormodus AP besteedt al zijn cycli aan het scannen van kanalen op zoek naar schurken en over-the-air aanvallen. Een monitor mode AP kan tegelijkertijd worden gebruikt voor adaptieve WIPS, locatie (context-bewuste) services en andere monitor mode services.

Wanneer AP's in de monitormodus worden geïmplementeerd, zijn de voordelen minder tijd voor detectie. Wanneer AP's in de monitormodus bovendien zijn geconfigureerd met adaptieve IPS, kan een bredere reeks aan over-the-air bedreigingen en aanvallen worden gedetecteerd.

AP's in lokale modus

Dient clients aan met off-channel scannen met tijdsnijden

Luistert voor 50 ms op elk kanaal

Configureerbaar voor scannen:

- Alle kanalen
- Landkanalen (standaard)
- DCA-kanalen

Monitormodus AP

Speciale scan

Luistert voor 1.2s op elk kanaal

Alle kanalen scannen

Identificatie van fraude

Als de respons van een sonde of de bakens van een schurkenapparaat worden gehoord door lokale, flex-connect of monitormodus AP's, dan wordt deze informatie via CAPWAP doorgegeven aan de Wireless LAN controller (WLC) voor het proces. Om fout-positieven te voorkomen, wordt een aantal methoden gebruikt om ervoor te zorgen dat andere beheerde op Cisco gebaseerde AP's niet worden geïdentificeerd als een bedrieglijk apparaat. Deze methodes omvatten mobiliteitsgroep updates, RF buurpakketten, en toegestane lijstvriendelijke AP's via Prime Infrastructuur (PI).

Rogue Records

Terwijl de database van de controller van schurkenapparaten alleen de huidige set van gedetecteerde schurken bevat, bevat de PI ook een gebeurtenisgeschiedenis en logt schurken die niet meer worden gezien.

Rogue Details

Een CAPWAP AP gaat 50 ms van het kanaal af om te luisteren op schurkenclients, monitor voor lawaai, en kanaalinterferentie. Alle gedetecteerde fraudeclients of AP's worden naar de controller verzonden, die deze informatie verzamelt:

- Het bedrieglijke AP MAC-adres
- Naam van het toegangspunt gedetecteerd
- Het MAC-adres van de frauduleuze verbonden client(s)
- Beveiligingsbeleid
- Inleiding
- De signaal-ruisverhouding (SNR)
- De indicator voor de signaalsterkte van de ontvanger (RSSI)
- Kanaal van schurkendetectie
- Radio waarin schurk wordt gedetecteerd

- Schurk SSID (als de schurk SSID wordt uitgezonden)
- Bedrieglijk IP-adres
- Eerste en laatste keer dat de schurk wordt gemeld
- Kanaalbreedte

Rogue-gebeurtenissen exporteren

Om frauduleuze gebeurtenissen naar een externe Network Management System (NMS) voor archivering te exporteren, maakt WLC het mogelijk om extra SNMP-trap-ontvangers toe te voegen. Wanneer een schurk wordt gedetecteerd of gewist door de controller, wordt een val die deze informatie bevat gecommuniceerd naar alle SNMP-trapontvangers. Een bezwaar met de export van gebeurtenissen via SNMP is dat als meerdere controllers dezelfde schurk detecteren, duplicate gebeurtenissen worden gezien door de NMS omdat correlatie alleen wordt gedaan bij PI.

Time-out bij Rogue Record

Zodra een schurk AP is toegevoegd aan de WLC records, blijft het er tot het niet meer wordt gezien. Na een door de gebruiker configureerbare timeout (1200 seconden standaard), wordt een schurk in de **_unclassification_category** verouderd.

Schurken in andere toestanden zoals **_Contained_and_Friendly_** persisteren zodat de juiste classificatie op hen wordt toegepast als ze weer verschijnen.

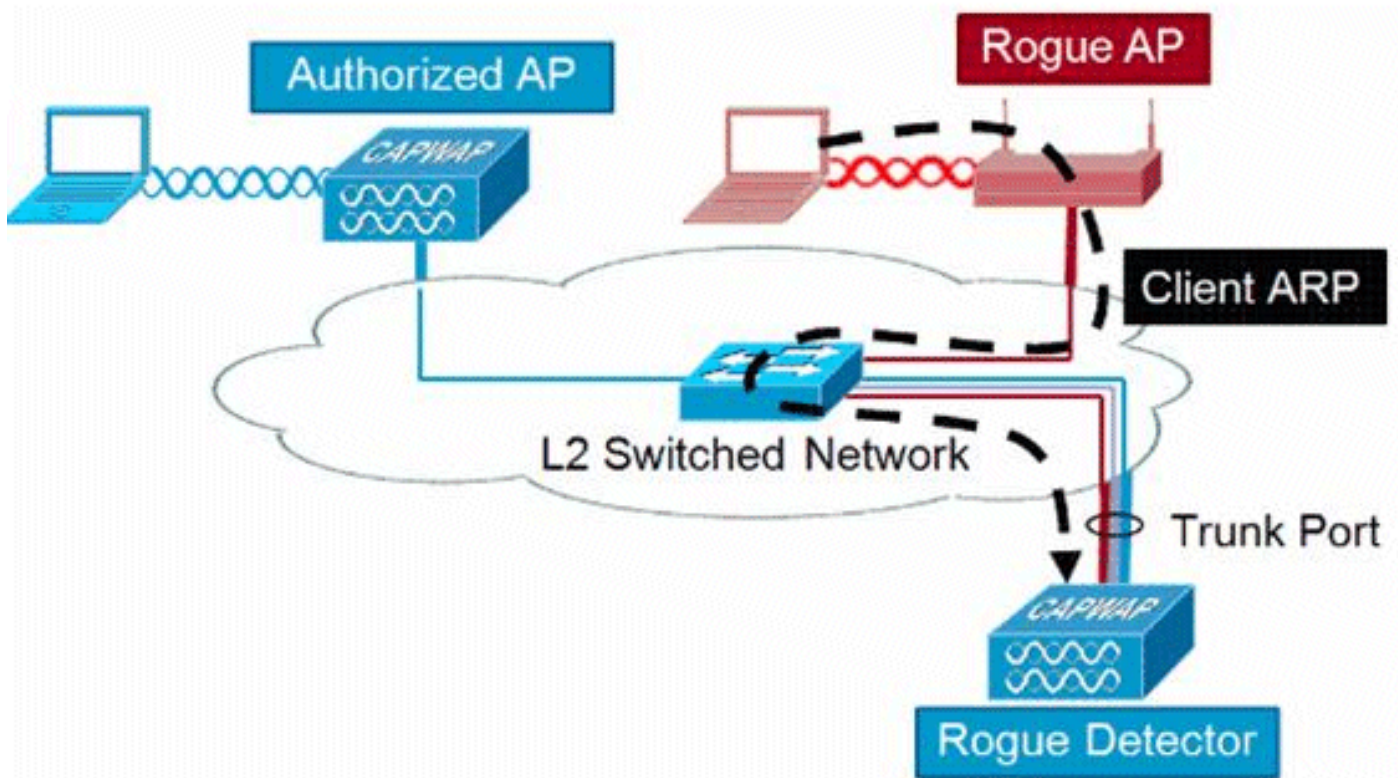
Er is een maximale databasegrootte voor schurkenrecords die variabel is tussen besturingsplatformen:

- 3504 - Detectie en insluiting van maximaal 600 Rogue AP's en 1500 Rogue Clients
- 5520 - Detectie en insluiting van maximaal 24000 Rogue AP's en 32000 Rogue Clients
- 8540 - Detectie en insluiting van maximaal 24000 Rogue AP's en 32000 Rogue Clients

Schurfdetectie - AP

Een schurkendetector AP is bedoeld om schurkeninformatie die via de lucht wordt gehoord te correleren met ARP informatie die wordt verkregen uit het bekabelde netwerk. Als een MAC-adres via de ether wordt gehoord als een schurkenAP of -client en ook wordt gehoord op het bekabelde netwerk, dan wordt de schurk bepaald om op het bekabelde netwerk te zijn. Als de schurk wordt gedetecteerd om op het bekabelde netwerk te zijn, dan wordt de alarmernst voor dat schurkenAP verhoogd to **_critical_**. Een schurkendetector AP is niet succesvol bij de identificatie van schurkencliënten achter een apparaat dat NAT gebruikt.

Deze benadering wordt gebruikt wanneer bedrieglijke AP één of andere vorm van authenticatie, of WEP of WPA heeft. Wanneer een vorm van verificatie is geconfigureerd op frauduleuze AP, kan de lichtgewicht AP niet koppelen omdat het niet weet de verificatiemethode en referenties die zijn geconfigureerd op de frauduleuze AP.



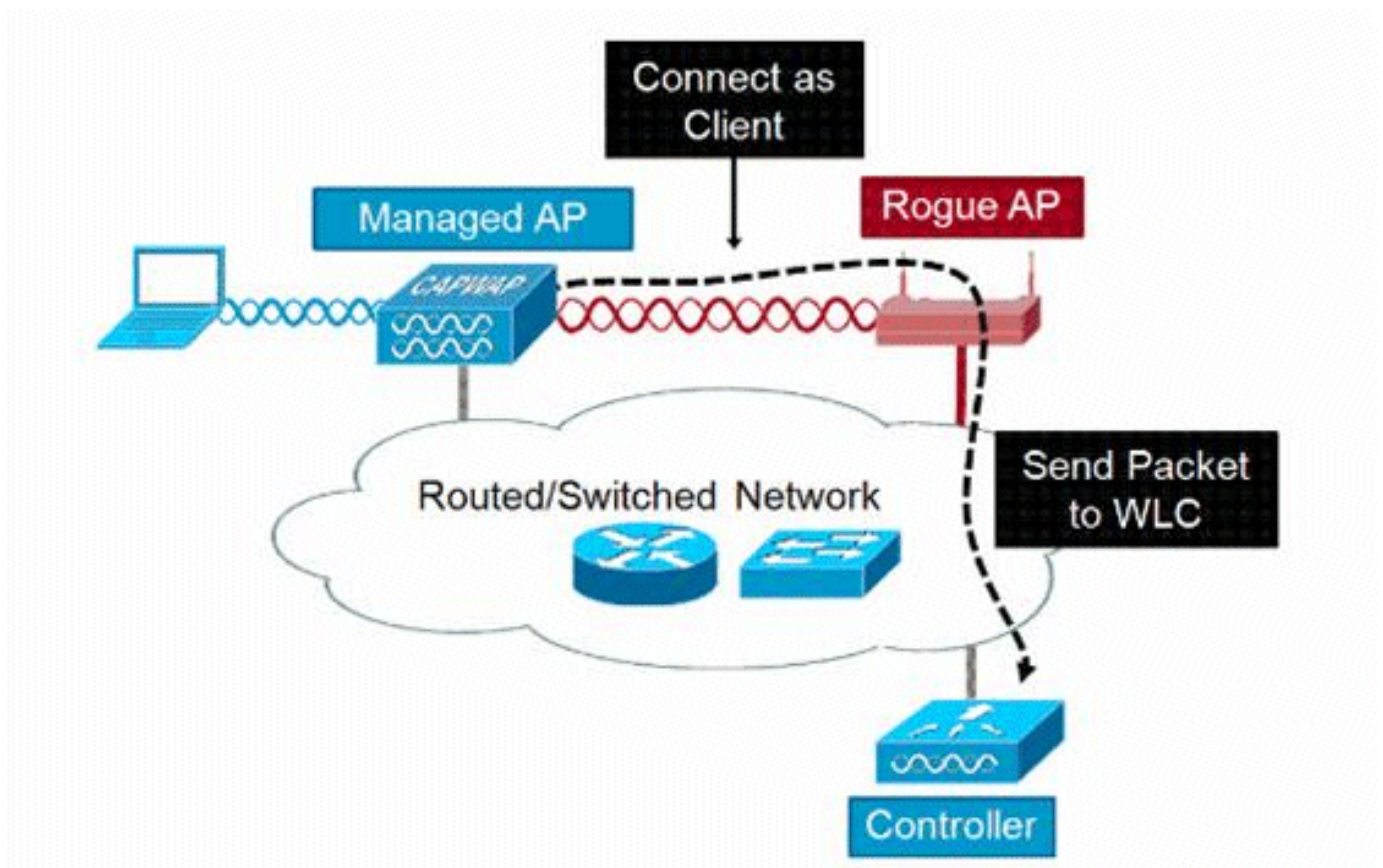
Opmerking: Alleen Wave 1 AP's kunnen worden geconfigureerd als Rogue Detectors.

schaalbaarheidsoverwegingen

Een schurkendetector AP kan tot 500 schurken en 500 schurkencliënten ontdekken. Als de schurkendetector wordt geplaatst op een stam met te veel schurkenapparaten, dan worden deze limieten overschreden, wat problemen veroorzaakt. Houd bedrieglijke detectie-AP's op de distributie- of toegangslaag van uw netwerk om te voorkomen dat dit gebeurt.

RLDP

Het doel van RLDP is te identificeren als een specifieke schurkenAP met de bedrade infrastructuur wordt verbonden. Deze eigenschap gebruikt hoofdzakelijk het dichtste AP om met het schurkenapparaat als draadloze cliënt te verbinden. Na de verbinding als client wordt een pakket verzonden met het doeladres van de WLC om te beoordelen of de AP is verbonden met het bekabelde netwerk. Als de schurk wordt gedetecteerd om op het bekabelde netwerk te zijn, dan wordt de alarm ernst voor die schurkenAP verhoogd naar kritisch.



Het algoritme van RLDP wordt hier vermeld:

1. Identificeer het dichtste Unified AP bij de schurk door het gebruik van de waarden van de signaalsterkte.
2. AP verbindt dan met de schurk als WLAN-client, probeert drie associaties voordat het keer uit.
3. Als de associatie succesvol is, gebruikt het toegangspunt DHCP om een IP-adres te verkrijgen.
4. Als een IP-adres is verkregen, stuurt het toegangspunt (dat optreedt als WLAN-client) een UDP-pakket naar elk van de IP-adressen van de controllers.
5. Als de controller ook maar één van de RLDP-pakketten van de client ontvangt, wordt die schurk gemarkeerd als on-wire met een kritische ernst.

Opmerking: De RLDP-pakketten kunnen de controller niet bereiken als de filterregels zijn ingesteld tussen het controllernetwerk en het netwerk waar het fraudeapparaat zich bevindt.

Voorbehouden bij RLDP

- RLDP werkt alleen met open frauduleuze AP's die hun SSID uitzenden met authenticatie en encryptie uitgeschakeld.
- RLDP vereist dat beheerde AP die als client optreedt een IP-adres via DHCP op het schurkennetwerk kan verkrijgen
- Handmatige RLDP kan worden gebruikt om meerdere malen te proberen en RLDP-sporen op een schurk.
- Tijdens het RLDP-proces kan het toegangspunt geen clients bedienen. Dit heeft een

negatieve invloed op de prestaties en connectiviteit van toegangspunten met de lokale modus.

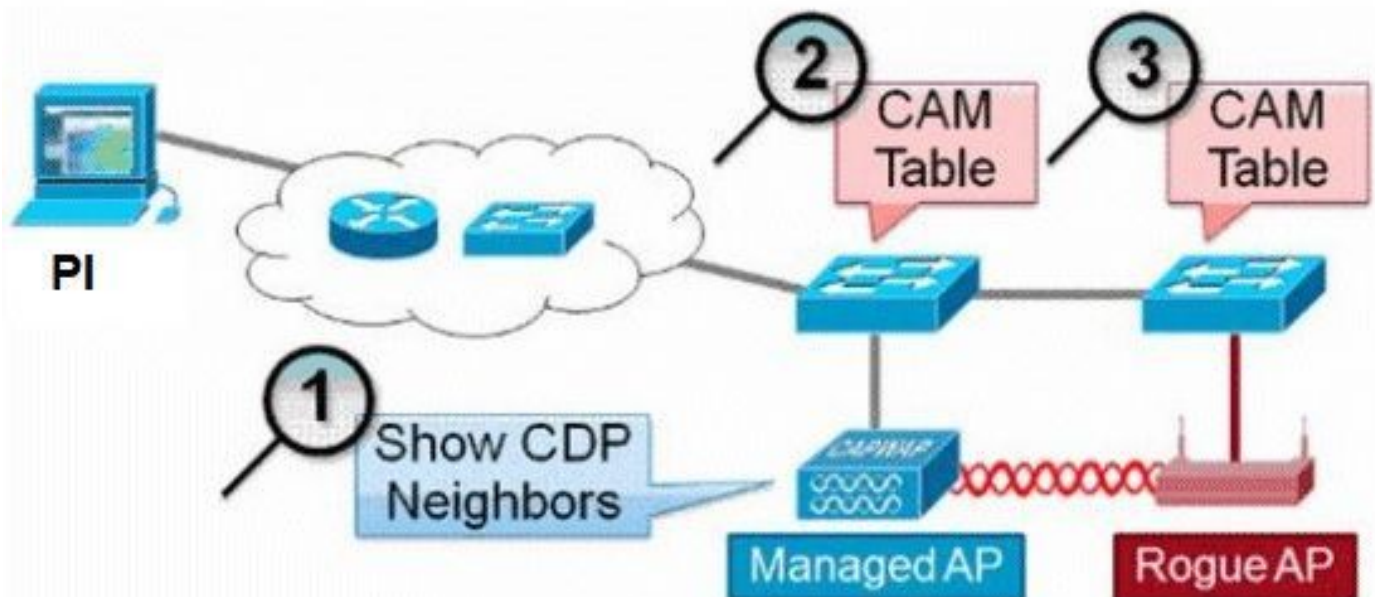
- RLDP probeert geen verbinding te maken met een frauduleuze AP die werkt met een 5 GHz DFS-kanaal.

Switch-poortsporen

Switch poort spoor is een schurk AP matiging techniek. Hoewel de switch-poorttracering wordt gestart bij de IP, wordt zowel CDP- als SNMP-informatie gebruikt om een route naar een specifieke poort in het netwerk te volgen.

Opdat de switch port trace kan worden uitgevoerd, moeten alle switches in het netwerk aan de IP met SNMP-referenties worden toegevoegd. Hoewel alleen-lezen referenties werken om de poort te identificeren waarop de schurk is ingeschakeld, laten lees-schrijfreferenties toe dat de IP ook de poort uitschakelt, dus bevat het de bedreiging.

Op dit moment werkt deze functie alleen met Cisco-switches waarop Cisco IOS® met CDP is ingeschakeld en moet CDP ook zijn ingeschakeld op de beheerde AP's.



Het algoritme voor het switch poortspoor wordt hier vermeld:

1. De PI vindt het dichtste AP, die de schurkenAP over-the-air detecteert, en haalt zijn CDP burens terug.
2. De PI gebruikt dan SNMP om de CAM-tabel binnen de buurman switch te onderzoeken, het zoekt naar een positieve match om de rogues locatie te identificeren.
3. Een positieve match is gebaseerd op het exacte MAC-adres, +1/-1 het MAC-adres van de schurk, enige MAC-adressen van de schurkenclient, of een OUI-match gebaseerd op de informatie van de verkoper inherent aan een MAC-adres.
4. Als een positieve overeenkomst niet op de dichtste switch wordt gevonden, zet IP het onderzoek in buurhop switches tot twee hop weg (door gebrek) voort.

Wired-Side Tracing Techniques

Comparison

	How it Works	What It Detects	Accuracy
Switchport Tracing	<ol style="list-style-type: none"> 1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port 	<ul style="list-style-type: none"> • Open APs • Secured APs • NAT APs 	<ul style="list-style-type: none"> • Moderate
RLDP	<ol style="list-style-type: none"> 1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire 	<ul style="list-style-type: none"> • Open APs • NAT APs 	<ul style="list-style-type: none"> • 100%
Rogue Detector	<ol style="list-style-type: none"> 1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs 	<ul style="list-style-type: none"> • Open APs • Secured APs • NAT APs 	<ul style="list-style-type: none"> • High

Schurkenclassificatie

Standaard worden alle talen die door het UWN van Cisco worden gedetecteerd, als niet-geclassificeerd beschouwd. Zoals in deze afbeelding wordt getoond, kunnen schurken worden geclassificeerd op basis van een aantal criteria, zoals RSSI, SSID, beveiligingstype, aan/uit-netwerk en aantal clients:



Schurkenclassificatieregels

Schurkenclassificatieregels, staat u toe om een reeks voorwaarden te bepalen die een schurk als of kwaadwillig of vriendelijk merken. Deze regels worden ingesteld bij de PI of de WLC, maar ze worden altijd uitgevoerd op de controller als nieuwe schurken worden ontdekt.

Lees de op [documentregel gebaseerde schurkenclassificatie in draadloze LAN-controllers \(WLC\) en Prime Infrastructure \(PI\)](#) voor meer informatie over schurkenregels in de WLC's.

HA Feiten

Als u handmatig een schurkenapparaat naar een ingesloten toestand (een klasse) of vriendelijke toestand verplaatst, wordt deze informatie opgeslagen in het standby Cisco WLC-flitsgeheugen; de gegevensbank wordt echter niet bijgewerkt. Wanneer HA switchover optreedt, wordt de schurkenlijst van het voorheen standby Cisco WLC-flitsgeheugen geladen.

In een scenario met hoge beschikbaarheid, als het beveiligingsniveau van de schurkendetectie is ingesteld op Hoog of Kritisch, begint de schurkentimer op de standby-controller pas na de schurkendetectie pend stabilisatietijd, die 300 seconden is. Daarom worden de actieve configuraties op de standby controller pas na 300 seconden weergegeven.

Flex-Connect - feiten

Een FlexConnect AP (met fraudedetectie ingeschakeld) in de aangesloten modus neemt de insluitingslijst van de controller. Als de optie SSID automatisch bevatten en Adhoc-instellingen automatisch worden ingesteld in de controller, worden deze configuraties ingesteld op alle FlexConnect-toegangspunten in de aangesloten modus en slaat het toegangspunt het in zijn geheugen op.

Wanneer het FlexConnect-toegangspunt naar een standalone modus verplaatst, worden de volgende taken uitgevoerd:

- De door de controller ingestelde insluiting gaat door.
- Als FlexConnect AP een bedrieglijke AP detecteert met dezelfde SSID als die van infra SSID (SSID geconfigureerd in de controller waar FlexConnect AP op is aangesloten), dan wordt de insluiting gestart als de auto SSID was ingeschakeld van de controller voordat het zich verplaatst naar de standalone modus.
- Als het FlexConnect-toegangspunt een ad-hocschurk detecteert, wordt de insluiting gestart als de automatische insluiting van de adhoc-controller was ingeschakeld toen die zich in de verbonden modus bevond.

Wanneer het zelfstandige FlexConnect-toegangspunt zich weer in de aangesloten modus beweegt, worden de volgende taken uitgevoerd:

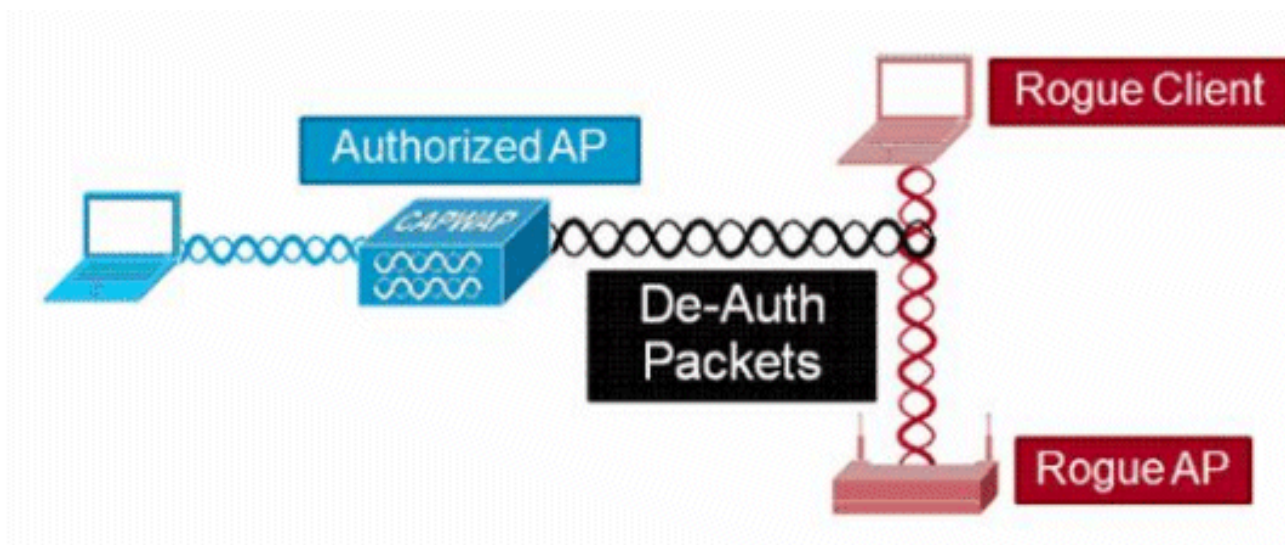
- Alle beperkingen worden gewist.
- Ingesloten die van de controlemechanisme wordt geïnitieerd neemt over.

Kreukvrij

Schurkenbeperking

Insluiting is een methode waarbij gebruik wordt gemaakt van over-the-air pakketten om tijdelijk de

service op een schurkenapparaat te onderbreken totdat het fysiek kan worden verwijderd. Insluiting werkt met de parodie van de-authenticatie pakketten met het spoofed bronadres van de schurk AP, zodat alle bijbehorende clients worden uitgeschakeld.



Details van Rogue Containment

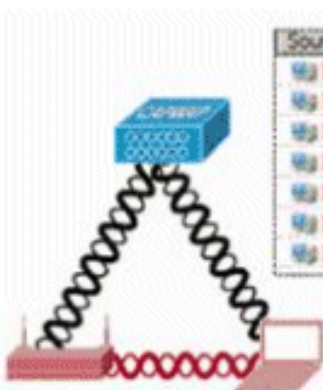
Een insluiting die op een frauduleuze AP zonder cliënten wordt geïnitieerd gebruikt slechts de-authenticatiekaders die naar het uitzendingsadres worden verzonden:



Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth

Broadcast Deauth frames only

Een inperking die op een frauduleuze AP wordt geïnitieerd met client(s) gebruikt de-authenticatie frames die naar het uitzendadres en naar het client(s) adres worden verzonden:




Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth

Broadcast and Unicast Deauth frames

Insluitingspakketten worden verzonden op het energieniveau van het beheerde toegangspunt en met de laagste gegevensnelheid.

De insluiting verzendt een minimum van 2 pakketten elke 100ms:

Source	Destination	De...	Size	Relative Time	Protocol
W Rogue AP	Ethernet Broadcast	6.0	56	0.000000	802.11 Deauth
W Rogue AP	Ethernet Broadcast	6.0	30	0.000004	802.11 Deauth
W Rogue AP	Ethernet Broadcast	6.0	144	0.000007	802.11 Beacon
W Rogue AP	Ethernet Broadcast	6.0	56	0.102414	802.11 Deauth
W Rogue AP	Ethernet Broadcast	6.0	30	0.102419	802.11 Deauth



Opmerking: Een insluiting die wordt uitgevoerd door AP's die geen monitormodus hebben, wordt verzonden met een interval van 500 ms in plaats van het interval van 100 ms dat wordt gebruikt door AP's in de monitormodus.

- Een individueel schurkenapparaat kan worden ingesloten door 1 tot 4 beheerde AP's die samenwerken om de dreiging tijdelijk te verminderen.
- Inperking kan worden uitgevoerd door gebruik te maken van lokale modus, monitormodus en flex-connect (Connected) modus, AP's. Voor lokale modus van flex-connect AP's kunnen maximaal drie fraudeapparaten per radio worden ingesloten. Voor monitormodus AP's kunnen maximaal zes fraudeapparaten per radio worden ingesloten.

Automatische insluiting

Naast het handmatig initiëren van insluiting op een schurkenapparaat via PI of de WLC GUI, is er ook de mogelijkheid om insluiting automatisch te starten onder bepaalde scenario's. Deze configuratie is te vinden onder Generalin de sectie **Rogue Policy** van de PI of controller interface. Elk van deze functies is standaard uitgeschakeld en kan alleen worden ingeschakeld om de bedreigingen die de meeste schade veroorzaken, ongedaan te maken.

- Scheur op draad - Als een schurkenapparaat wordt geïdentificeerd om aan het bekabelde netwerk te worden bevestigd, wordt het automatisch onder insluiting geplaatst.
- Gebruik van onze SSID - Als een bedrieglijk apparaat een SSID gebruikt die hetzelfde is als dat ingesteld is op de controller, is het automatisch ingesloten. Deze functie is bedoeld om een honingpot-aanval aan te pakken voordat het schade veroorzaakt.
- Geldige client op Rogue AP - Als een client die in Radius/AAA-server vermeld staat blijkt te zijn geassocieerd met een schurkenapparaat, wordt insluiting alleen gestart tegen die client, voorkomt dit dat deze wordt gekoppeld aan een niet-beheerd AP.
- AdHoc Rogue AP - Als een ad-hocnetwerk wordt ontdekt, is het automatisch ingesloten.

Voorbehouden bedriegers

- Omdat de insluiting een deel van de radiotijd van de beheerde AP gebruikt om de de-authenticatie frames te verzenden, worden de prestaties aan zowel gegevens als spraakclients negatief beïnvloed door tot 20%. Voor gegevensclients wordt de doorvoersnelheid verlaagd. Voor stemcliënten, kan de insluiting onderbrekingen in gesprekken en verminderde stemkwaliteit veroorzaken.
- Inperking kan juridische gevolgen hebben wanneer deze tegen netwerken in de buurlanden wordt gelanceerd. Zorg ervoor dat het bedrieglijke apparaat binnen uw netwerk is en een veiligheidsrisico vormt alvorens u de insluiting lanceert.

Switch Port Shut

Zodra een switch poort wordt getraceerd door het gebruik van SPT, is er een mogelijkheid om die poort in PI uit te schakelen. De beheerder moet dit handmatig doen. Er is een optie om de switch via IP in te schakelen als de schurk fysiek uit het netwerk wordt verwijderd.

Configureren

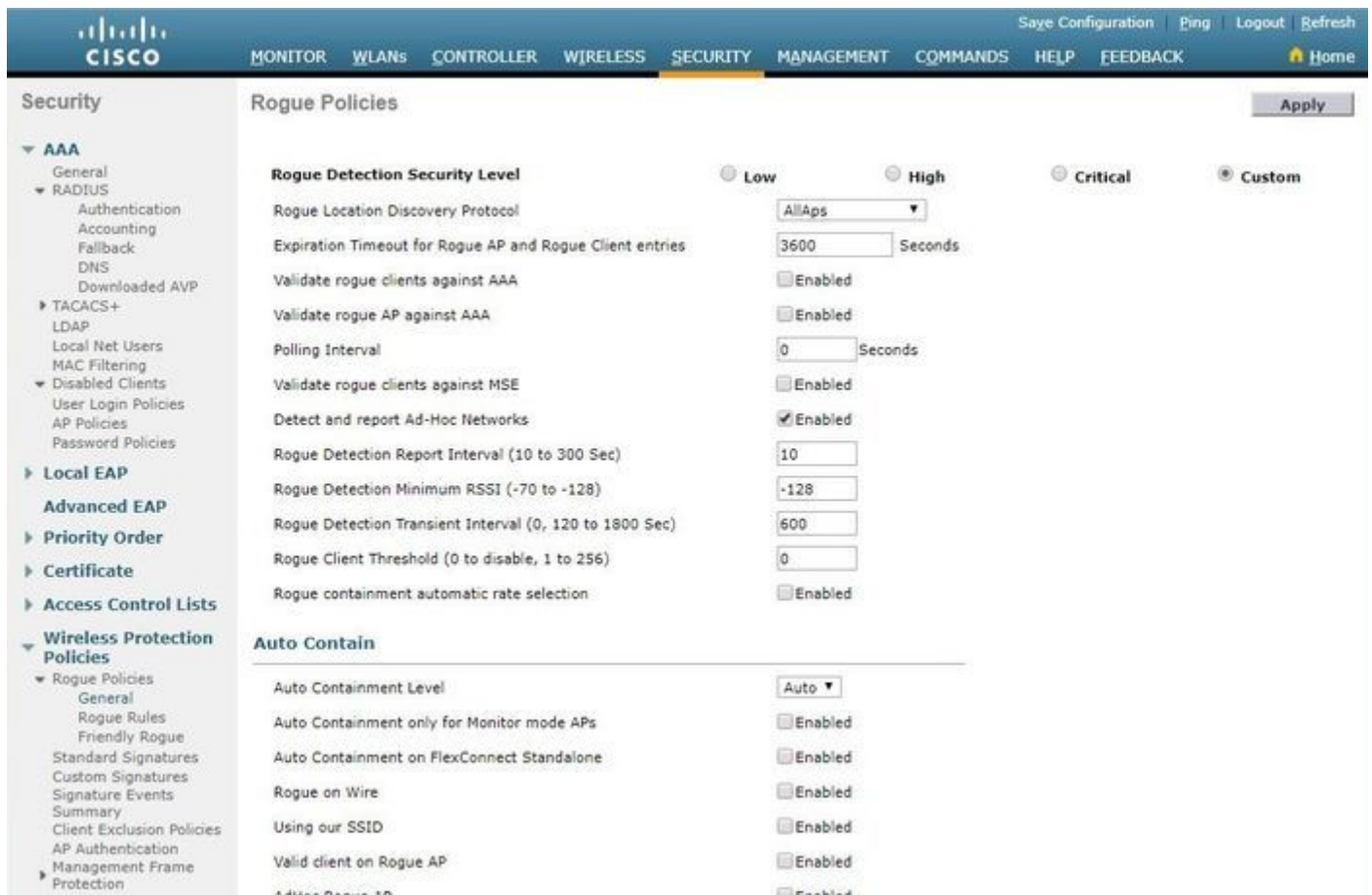
Schurfdetectie configureren

Schurfdetectie is standaard ingeschakeld in de controller.

Als u verschillende opties wilt configureren, navigeert u naar **Security > Wireless Protection Policies > Rogue Policies > General**. Bijvoorbeeld:

Stap 1. Wijzig de tijd voor frauduleuze AP's.

Stap 2. Schakel de detectie van ad-hocschurkennetwerken in.



The screenshot shows the Cisco WLC configuration interface for Rogue Policies. The 'Rogue Policies' section is expanded, showing the following settings:

- Rogue Detection Security Level:** Radio buttons for Low, High, Critical, and Custom (selected).
- Rogue Location Discovery Protocol:** AllAps (dropdown)
- Expiration Timeout for Rogue AP and Rogue Client entries:** 3600 Seconds
- Validate rogue clients against AAA:** Disabled
- Validate rogue AP against AAA:** Disabled
- Polling Interval:** 0 Seconds
- Validate rogue clients against MSE:** Disabled
- Detect and report Ad-Hoc Networks:** Enabled (checked)
- Rogue Detection Report Interval (10 to 300 Sec):** 10
- Rogue Detection Minimum RSSI (-70 to -128):** -128
- Rogue Detection Transient Interval (0, 120 to 1800 Sec):** 600
- Rogue Client Threshold (0 to disable, 1 to 256):** 0
- Rogue containment automatic rate selection:** Disabled

The 'Auto Contain' section shows the following settings:

- Auto Containment Level:** Auto (dropdown)
- Auto Containment only for Monitor mode APs:** Disabled
- Auto Containment on FlexConnect Standalone:** Disabled
- Rogue on Wire:** Enabled
- Using our SSID:** Enabled
- Valid client on Rogue AP:** Enabled
- AdHoc Rogue AP:** Enabled

Van de CLI:

```
(Cisco Controller) >config rogue ap timeout ?
```

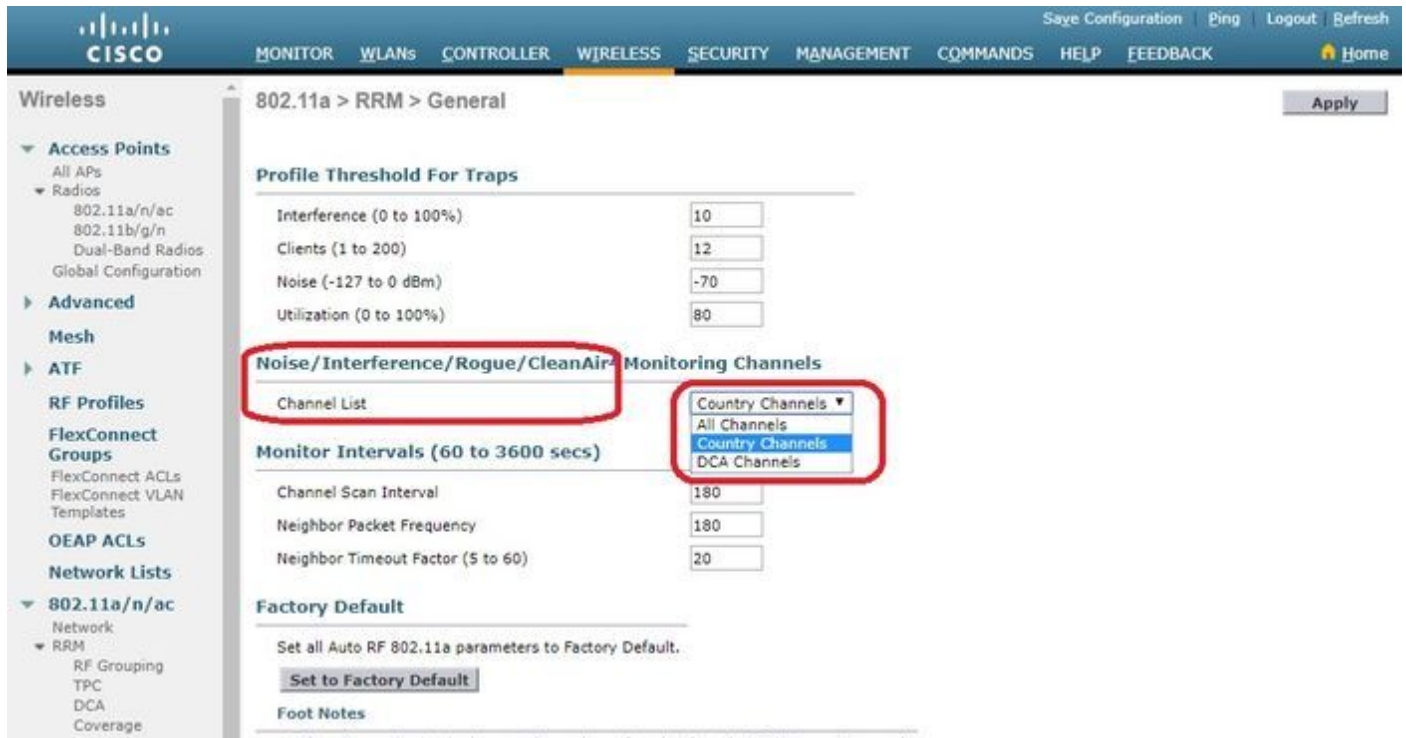
```
<seconds> The number of seconds<240 - 3600> before rogue entries are flushed
```

```
(Cisco Controller) >config rogue adhoc enable/disable
```

Kanaalscan configureren voor detectie van fouten

Voor een lokale/Flex-Connect/Monitor modus AP is er een optie onder RRM configuratie die de gebruiker in staat stelt om te kiezen welke kanalen gescand zijn voor kwaden. Het hangt af van de configuratie, de AP scant alle kanaal/land kanaal/DCA kanaal voor schurken.

Als u dit via de GUI wilt configureren, navigeert u naar **Wireless > 802.11a/802.11b > RM > Algemeen**, zoals in de afbeelding.



Van de CLI:

```
(Cisco Controller) >config advanced 802.11a monitor channel-list ?
```

```
all           Monitor all channels
country       Monitor channels used in configured country code
dca           Monitor channels used by automatic channel assignment
```

Schurkenclassificatie configureren

Handmatig een bedrieglijke AP classificeren

Als u een bedrieglijke AP als vriendelijk, kwaadaardig of niet geclassificeerd wilt classificeren, navigeer dan naar **Monitor > Rogue > Niet-geclassificeerde AP's** en klik op de specifieke bedrieglijke AP-naam. Kies de optie uit de vervolgkeuzelijst, zoals in de afbeelding.

Rogue AP Detail

MAC Address: 00:06:91:43:6d:e2

Type: AP

Is Rogue On Wired Network?: No

First Time Reported On: Thu May 30 16:21:30 2019

Last Time Reported On: Fri May 31 13:07:11 2019

Class Type: **Malicious** (dropdown menu)

State: (dropdown menu)

Manually Contained: No

Update Status: -- Choose New Status --

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	Security Policy	Pre-A
b4:de:31:c6:30:c0	AP2800-1	Cisco-17D90F4C	6	20	802.11n2.4G	Open	Long

Van de CLI:

(Cisco Controller) > **config rogue ap ?**

```

classify          Configures rogue access points classification.
friendly          Configures friendly AP devices.
rldp              Configures Rogue Location Discovery Protocol.
ssid              Configures policy for rogue APs advertsing our SSID.
timeout           Configures the expiration time for rogue entries, in seconds.
valid-client      Configures policy for valid clients which use rogue APs.
  
```

Om een bedrieglijke ingang uit de bedrieglijke lijst manueel te verwijderen, navigeer aan **Monitor > Schurk > Niet geclassificeerde APs**, en klik **Remove**, zoals aangetoond in het beeld.

Unclassified Rogue APs

Current Filter: None [Change Filter] [Clear Filter]

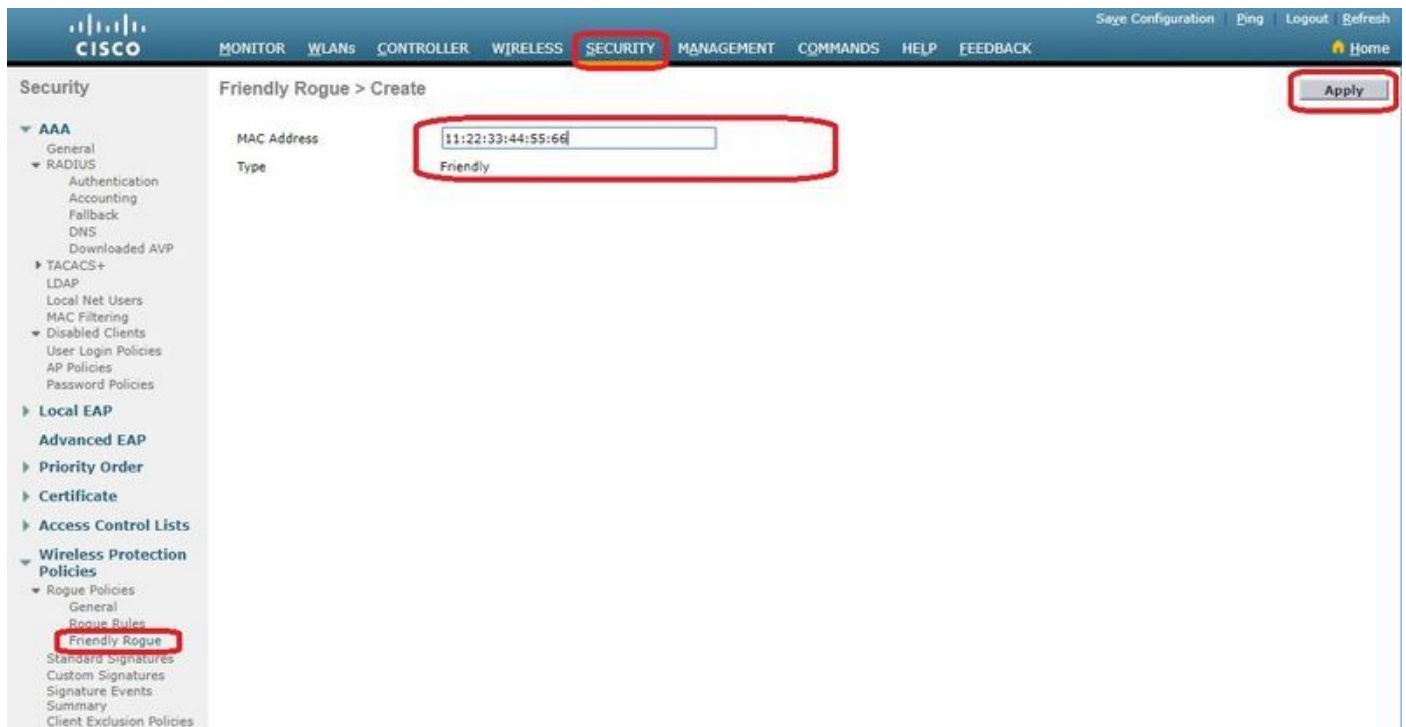
Remove, Contain, Move to Alert

MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:06:91:43:6d:e2	Cisco-17D90F4C	6	1	0	Alert
00:1a:2b:58:6b:13	NUMERICABLE-29F3	6	1	0	Alert
00:22:ce:ff:38:aa	S7afb7	11	1	0	Alert
00:22:ce:ff:47:5a	d9b9a9	Unknown	0	0	Alert
00:23:be:30:59:18	368a98	11	1	0	Alert
00:23:be:51:85:01	eb4fb0	11	1	0	Alert

Om een Rogue AP te configureren als een vriendelijke AP, navigeer naar **Security > Wireless Protection Policies > Rogue Policies > Friendly Rogues** en voeg het frauduleuze MAC-adres toe.

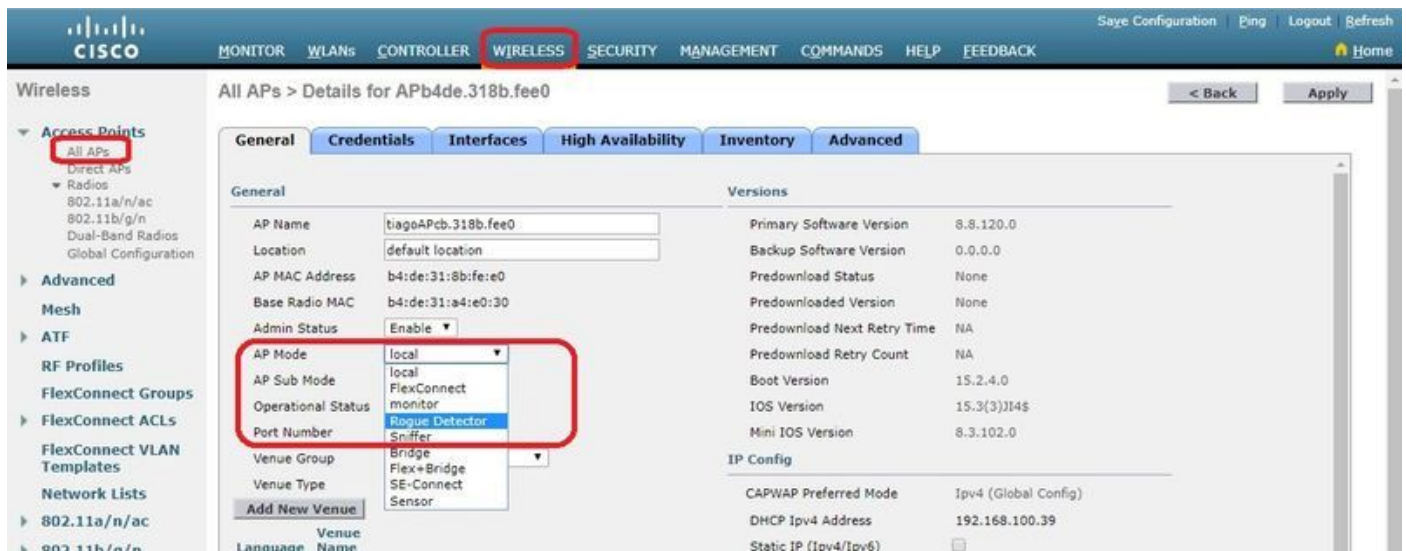
De toegevoegde vriendelijke schurkenvermeldingen kunnen worden geverifieerd **van Monitor >**

Rogues > Friendly Roguepage, zoals getoond in de afbeelding.



SchuifdetectorAP configureren

Als u het toegangspunt wilt configureren als een fraudedetector via de GUI, navigeert u naar Wireless > Alle toegangspunten. Kies de naam van het toegangspunt en wijzig de modus van het toegangspunt zoals in de afbeelding.



Van de CLI:

```
(Cisco Controller) >config ap mode rogue AP_Managed
```

```
Changing the AP's mode cause the AP to reboot.  
Are you sure you want to continue? (y/n) y
```

Switchpoort configureren voor een detectie van mazen AP

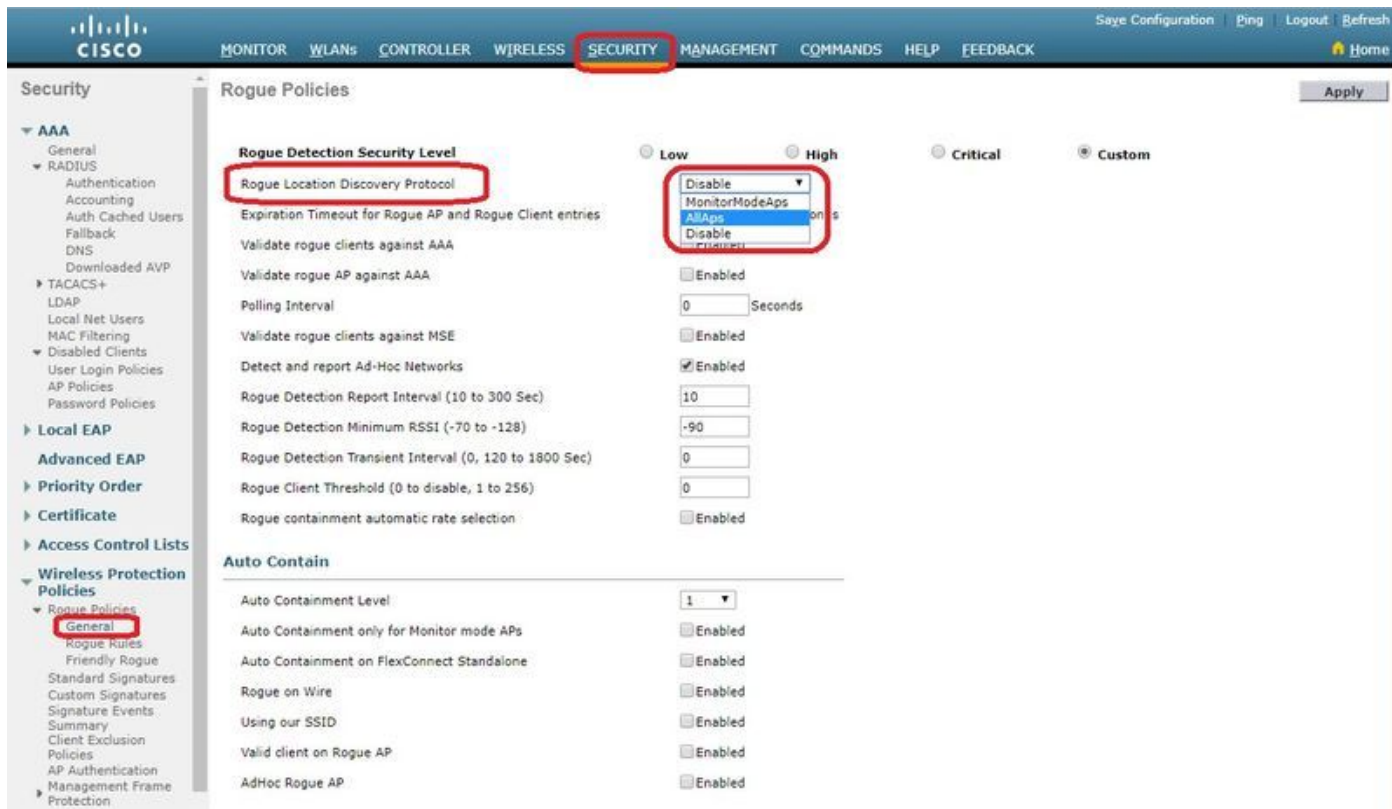
```
interface GigabitEthernet1/0/5
```

description Rogue Detector
switchport trunk native vlan 100
switchport mode trunk

Opmerking: Inheems VLAN in deze configuratie is één die IP connectiviteit aan WLC heeft.

RLDP configureren

Als u RLDP wilt configureren in de GUI van de controller, gaat u naar **Security > Wireless Protection Policies > Rogue Policies > General**.



Monitormodus AP's - hiermee kunnen alleen AP's in monitormodus deelnemen aan RLDP.

Alle AP's - Local/Flex-Connect/Monitor mode AP's nemen deel aan het RLDP-proces.

Uitgeschakeld - RLDP wordt niet automatisch geactiveerd. De gebruiker kan echter RLDP handmatig activeren voor een bepaald MAC-adres via de CLI.

Opmerking: AP met monitormodus krijgt de voorkeur boven lokale/Flex-Connect AP om RLDP uit te voeren als beide een bepaalde schurk boven -85 dbm RSSI detecteren.

Van de CLI:

```
(Cisco Controller) >config rogue ap rldp enable ?
```

alarm-only Enables RLDP and alarm if rogue is detected

auto-contain Enables RLDP, alarm and auto-contain if rogue is detected.

```
(Cisco Controller) >config rogue ap rldp enable alarm-only ?
```

monitor-ap-only Perform RLDP only on monitor AP

RLDP-schema en handmatig starten kunnen alleen worden geconfigureerd via opdrachtprompt.
RLDP handmatig starten:

```
(Cisco Controller) >config rogue ap rldp initiate ?
```

<MAC addr> Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).

Voor het schema van RLDP:

```
(Cisco Controller) >config rogue ap rldp schedule ?
```

add	Enter the days when RLDP scheduling to be done.
delete	Enter the days when RLDP scheduling needs to be deleted.
enable	Configure to enable RLDP scheduling.
disable	Configure to disable RLDP scheduling.

```
(Cisco Controller) >config rogue ap rldp schedule add ?
```

fri	Configure Friday for RLDP scheduling.
sat	Configure Saturday for RLDP scheduling.
sun	Configure Sunday for RLDP scheduling.
mon	Configure Monday for RLDP scheduling.
tue	Configure Tuesday for RLDP scheduling.
wed	Configure Wednesday for RLDP scheduling.
thu	Configure Thursday for RLDP scheduling.

RLDP-herhalingen kunnen met de opdracht worden geconfigureerd:

```
(Cisco Controller) >config rogue ap rldp retries ?
```

<count> Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.

Kreukvrij configureren

Handmatige insluiting instellen

Om een bedrieglijke AP handmatig te bevatten, navigeer naar **Monitor > Rogues > Unclassificeerd**, zoals in de afbeelding.

The screenshot shows the Cisco WLC Monitor interface. The 'MONITOR' tab is selected. The left sidebar shows the navigation menu with 'Unclassified APs' highlighted. The main content area displays 'Rogue AP Detail' for MAC Address 00:06:91:53:3a:20. The 'Update Status' dropdown is set to 'Contain'. A table below shows 'APs that detected this Rogue' with columns for Base Radio MAC, AP Name, SSID, and RSSI.

Base Radio MAC	AP Name	SSID	RSSI
00:27:e3:36:4d:a0	tiagoAPcb.90E1.3DEC		-128

Van de CLI:

(Cisco Controller) >**config rogue client** ?

aaa Configures to validate if a rogue client is a valid client which uses AAA/local database.
 alert Configure the rogue client to the alarm state.
 contain Start to contain a rogue client.
 delete Delete rogue Client
 mse Configures to validate if a rogue client is a valid client which uses MSE.

(Cisco Controller) >**config rogue client contain 11:22:33:44:55:66** ?

<num of APs> Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].

Opmerking: Een bepaalde schurk kan met 1-4 APs worden bevat. Standaard gebruikt de controller één AP om een client te bevatten. Als twee APs een bepaalde schurk kunnen ontdekken, bevat AP met hoogste RSSI de cliënt ongeacht de AP wijze.

Automatische insluiting

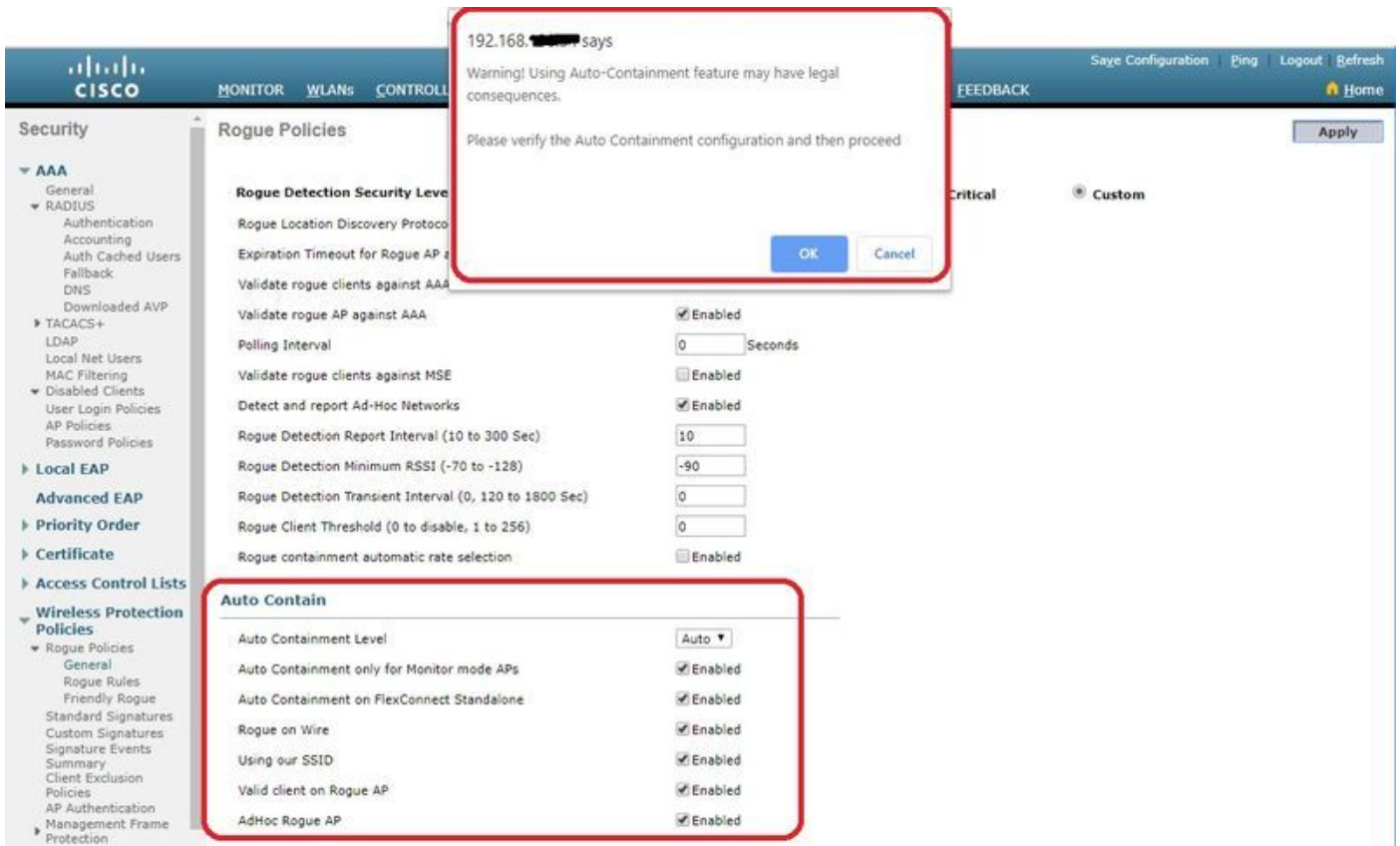
Als u automatische insluiting wilt configureren, gaat u naar **Security>Wireless Protection Policies>schurkenbeleid>Algemeen** en schakelt u alle toepasbare opties voor uw netwerk in.

Als u wilt dat Cisco WLC automatisch bepaalde schurkenapparaten bevat, schakelt u deze selectievakjes in. Anders laat u de selectievakjes niet ingeschakeld. Dit is de standaardwaarde.

Waarschuwing: Wanneer u een van deze parameters inschakelt, verschijnt het bericht:"Het gebruik van deze functie heeft juridische gevolgen. Wilt u doorgaan?" De 2.4- en 5-GHz frequenties in de Industrial, Scientific, and Medical (ISM)-band zijn toegankelijk voor het publiek en kunnen zonder licentie worden gebruikt. Als zodanig kan de insluiting van apparaten op het netwerk van een andere partij juridische gevolgen hebben.

Dit zijn de parameters voor automatisch bevatten:

Parameter	Beschrijving
Automatisch insluitingsniveau	<p>Drop-down lijst waaruit u de schurkenauto inperkingsniveau van 1 tot 4 kunt kiezen.</p> <p>U kunt maximaal vier AP's kiezen voor automatische insluiting wanneer een schurk naar een ingesloten staat wordt verplaatst via een van de automatische insluiting beleid.</p> <p>U kunt ook Auto kiezen voor automatische selectie van het aantal AP's dat gebruikt wordt voor automatische insluiting. Cisco WLC kiest het gewenste aantal AP's op basis van de RSSI voor effectieve insluiting.</p> <p>De RSSI-waarde die aan elk insluitingsniveau is gekoppeld, is als volgt:</p> <ul style="list-style-type: none">• 1-0 tot -55 dBm• 2-75-55 dBm• 3 — -85 tot -75 dBm• 4 — minder dan -85 dBm
Auto Containment alleen voor access points voor monitormodus	<p>Schakel het selectievakje in dat u kunt selecteren om de monitormodus van de AP's in te schakelen voor automatische insluiting. De standaardinstelling is uitgeschakeld.</p>
Auto Containment op FlexConnect, standalone	<p>Schakel het selectievakje in dat u kunt selecteren om de automatische insluiting van FlexConnect AP's in de standalone modus in te schakelen. De standaardinstelling is uitgeschakeld. Wanneer de FlexConnect AP's in de standalone modus staan, kunt u alleen het beleid Inschakelen voor automatische insluiting van SID of Ad Hoc Rogue AP. De insluiting stopt nadat de standalone AP verbinding maakt met de Cisco WLC.</p>
Rogue on Wire	<p>Schakel het selectievakje in dat u de talen die worden gedetecteerd in het bekabelde netwerk automatisch wilt bevatten. De standaardinstelling is uitgeschakeld.</p>
Gebruik onze SSID	<p>Schakel het selectievakje in dat u automatisch die schurken bevat die de SSID van uw netwerk adverteren. Als u deze parameter niet selecteert, genereert Cisco WLC alleen een alarm wanneer een dergelijke schurk wordt gedetecteerd. De standaardinstelling is uitgeschakeld.</p>
Geldige client op Rogue AP	<p>Schakel het selectievakje in om automatisch een bedrieglijk access point te bevatten waaraan vertrouwde clients zijn gekoppeld. Als u deze parameter niet selecteert, genereert Cisco WLC alleen een alarm wanneer een dergelijke schurk wordt gedetecteerd. De standaardinstelling is uitgeschakeld.</p>
AdHoc Rogue AP	<p>Schakel het selectievakje in dat u ad-hocnetwerken automatisch wilt bevatten die door Cisco WLC zijn gedetecteerd. Als u deze parameter niet selecteert, genereert Cisco WLC alleen een alarm wanneer een dergelijk netwerk wordt gedetecteerd. De standaardinstelling is uitgeschakeld.</p>



Klik op Toepassen om gegevens naar Cisco WLC te verzenden, maar de gegevens worden niet bewaard over een voedingscyclus. deze parameters worden tijdelijk opgeslagen in vluchtig RAM.

Van de CLI:

```
(Cisco Controller) >config rogue adhoc ?
```

```
alert          Stop Auto-Containment, generate a trap upon detection of the
                adhoc rogue.
auto-contain   Automatically contain adhoc rogue.
contain        Start to contain adhoc rogue.
disable        Disable detection and reporting of Ad-Hoc rogues.
enable         Enable detection and reporting of Ad-Hoc rogues.
external       Acknowledge presence of a adhoc rogue.
```

```
(Cisco Controller) >config rogue adhoc auto-contain ?
```

```
(Cisco Controller) >config rogue adhoc auto-contain
Warning! Use of this feature has legal consequences
Do you want to continue(y/n) :y
```

Met Prime-infrastructuur

Cisco Prime Infrastructure kan worden gebruikt om een of meer controllers en bijbehorende AP's te configureren en te bewaken. Cisco IP heeft tools om de bewaking en controle van grote systemen te vergemakkelijken. Wanneer u Cisco IP in uw draadloze oplossing van Cisco gebruikt, bepalen controllers periodiek de client, het fraudetoegangspunt, de client voor het fraudetoegangspunt, de locatie van de radiofrequentie-ID (RFID) en slaan ze de locaties op in de Cisco IP-database.

Cisco Prime Infrastructure ondersteunt op regels gebaseerde classificatie en gebruikt de

classificatieregels die op de controller zijn geconfigureerd. De controller stuurt na deze gebeurtenissen vallen naar Cisco Prime Infrastructure:

- Als een onbekend toegangspunt zich voor het eerst naar de staat Friendly beweegt, stuurt de controller een val naar Cisco Prime Infrastructure alleen als de schurkenstaat Waarschuwing is. Het stuurt geen val als het onroerend goed **intern** of **extern** is.
- Als een invoegtoepassing wordt verwijderd nadat de time-out is verlopen, stuurt de controller een val naar Cisco Prime Infrastructuurforrogueaccess points die zijn gecategoriseerd als **boosaardig** (waarschuwing, bedreiging) of **niet-geclassificeerd** (waarschuwing). De controller verwijdert geen overzichtsvermeldingen met de herkenningsrechten: **Ingesloten**, **ingesloten hangende**, **interne**, en **externe**.

Verifiëren

Om schurkendetails in een controller in de grafische interface te vinden, navigeer naar **Monitor > Rogues**, zoals in de afbeelding.

MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:a3:8e:db:01:a0	blizzard	13	1	0	Alert
00:a3:8e:db:01:a1	Unknown	13	1	0	Alert
00:a3:8e:db:01:a2	Unknown	13	1	0	Alert
00:a3:8e:db:01:b1	Unknown	40	2	0	Alert
00:a3:8e:db:01:b2	Unknown	40	2	0	Alert
50:2f:a8:a2:0d:40	butterfly	11	1	0	Alert
9c:97:26:61:d2:79	MEO-61D279	Unknown	0	0	Alert
9c:97:26:61:d2:7a	MEO-WiFi	6	1	0	Alert
bc:22:05:ea:21:26	NOWO-A2121	1	1	0	Alert
c4:e9:84:c1:c8:90	MEO-50E3EC	6	1	0	Alert

Op deze pagina zijn verschillende classificaties voor schurken beschikbaar:

- Vriendelijke AP's - AP's die door de beheerder als vriendelijk zijn gemarkeerd.
- Kwaadaardige AP's - AP's die zijn geïdentificeerd als kwaadaardig via RLDP of schurkendetectie-AP.
- Aangepaste AP's - AP's die zijn geclassificeerd als Custom by Rogue Rules.
- Niet-geclassificeerde AP's - Standaard schurkenAP's worden in controller weergegeven als niet-geclassificeerde lijst.
- Rogue Clients - Clients verbonden met Rogue AP's.
- Adhoc Rogues - Adhoc schurkenclients.
- Rogue AP negeert lijst - Zoals vermeld door PI.

Opmerking: Als WLC en autonome AP worden beheerd door dezelfde IP, maakt WLC automatisch een lijst van deze autonome AP in Rogue AP negeer lijst. Er is geen extra configuratie vereist in WLC om deze functie in te schakelen.

Klik op een bepaalde schurkenvermelding om de details van die schurk te krijgen. Hier is een voorbeeld van een Rogue gedetecteerd op een bekabeld netwerk:

CISCO **MONITOR** WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh Home

Monitor Rogue AP Detail < Back Apply

Summary

- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
 - Friendly APs
 - Malicious APs**
 - Custom APs
 - Unclassified APs
 - Rogue Clients
 - Adhoc Rogues
 - Friendly Adhoc
 - Malicious Adhoc
 - Custom Adhoc
 - Unclassified Adhoc
 - Rogue AP ignore-list
- Clients
- Sleeping Clients
- Multicast
- Applications
- Lync
- Local Profiling
- Cloud Services

MAC Address: 50:2f:a8:a2:0a:60

Type: AP

Is Rogue On Wired Network?: Yes

First Time Reported On: Mon Jun 3 14:12:54 2019

Last Time Reported On: Tue Jun 4 12:15:25 2019

Class Type: Malicious

Classification Change By: Auto

State: Threat

State Change By: Auto

Manually Contained: No

Update Status: -- Choose New Status --

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	Security Policy	Pre-Ambble	RSSI
00:27:e3:36:4d:a0	tiagoAPcb.98E1.3DEC	butterfly	1	20	802.11n2.4G	WPA2/FT	Long	-63

[Clients associated to this Rogue AP](#)

Van de CLI:

(Cisco Controller) > **show rogue ap summary**

```
Rogue Detection Security Level..... custom
Rogue Pending Time..... 180 secs
Rogue on wire Auto-Contain..... Disabled
Rogue uses our SSID Auto-Contain..... Disabled
Valid client on rogue AP Auto-Contain..... Disabled
Rogue AP timeout..... 1200
Rogue Detection Report Interval..... 10
Rogue Detection Min Rssi..... -90
Rogue Detection Transient Interval..... 0
Rogue Detection Client Num Threshold..... 0
Validate rogue AP against AAA..... Enabled
Rogue AP AAA validation interval..... 0 secs
Total Rogues(AP+Ad-hoc) supported..... 600
Total Rogues classified..... 12
```

MAC Address	Class	State	#Det	#Rogue	#Highest	RSSI	#RSSI
#Channel	#Second Highest	#RSSI	#Channel	Aps	Clients	det-Ap	

00:a3:8e:db:01:a0	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:a1	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:a2	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:b0	Malicious	Threat	2	1	00:27:e3:36:4d:a0	-27	40
00:27:e3:36:4d:a0	-37	40					
00:a3:8e:db:01:b1	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
00:27:e3:36:4d:a0	-36	40					
00:a3:8e:db:01:b2	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
00:27:e3:36:4d:a0	-37	40					
50:2f:a8:a2:0a:60	Malicious	Threat	1	2	00:27:e3:36:4d:a0	-66	1
50:2f:a8:a2:0d:40	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-65	11

```

9c:97:26:61:d2:79 Unclassified Alert      1    0      00:27:e3:36:4d:a0 -89    6
ac:22:05:ea:21:26 Unclassified Alert      1    0      00:27:e3:36:4d:a0 -89   (1,5)
c4:e9:84:c1:c8:90 Unclassified Alert      1    0      00:27:e3:36:4d:a0 -89   (6,2)
d4:28:d5:da:e0:d4 Unclassified Alert      1    0      00:27:e3:36:4d:a0 -85   13

```

(Cisco Controller) > **show rogue ap detailed 50:2f:a8:a2:0a:60**

```

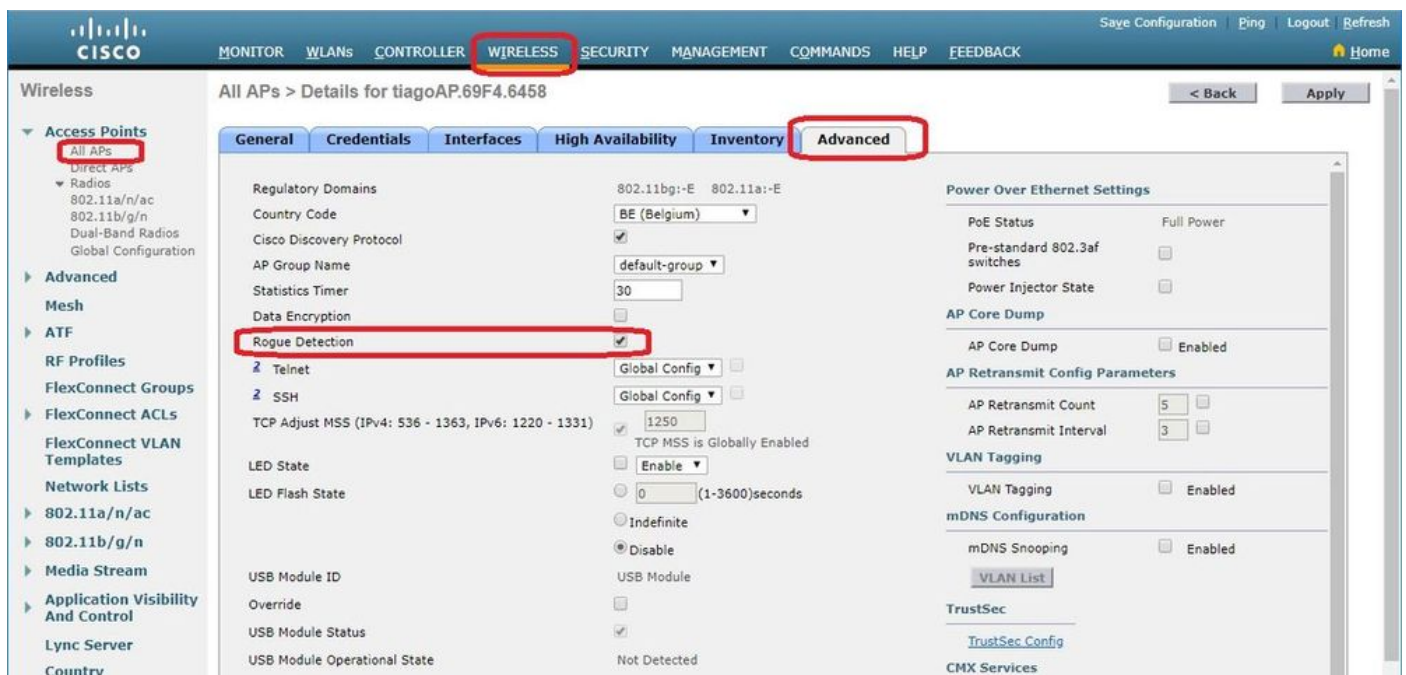
Rogue BSSID..... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network..... Yes
Classification..... Malicious
Classification change by..... Auto
Manual Contained..... No
State..... Threat
State change by..... Auto
First Time Rogue was Reported..... Tue Jun  4 13:06:55 2019
Last Time Rogue was Reported..... Wed Jun  5 08:25:57 2019
Reported By
  AP 1
    MAC Address..... 00:27:e3:36:4d:a0
    Name..... tiagoAPcb.98E1.3DEC
    Radio Type..... 802.11n2.4G
    SSID..... buterfly
    Channel..... 1
    RSSI..... -64 dBm
    SNR..... 29 dB
    Security Policy..... WPA2/FT
    ShortPreamble..... Disabled
    Last reported by this AP..... Wed Jun  5 08:25:57 2019

```

Problemen oplossen

Als de schurk niet wordt herkend

Controleer of bedrieglijke detectie is ingeschakeld op het toegangspunt. Op de GUI:



In de CLI:

```
(Cisco Controller) >show ap config general tiagoAPcb.98E1.3DEC

Cisco AP Identifier..... 13
Cisco AP Name..... tiagoAPcb.98E1.3DEC
[...]
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Disabled
AP SubMode ..... Not Configured
Rogue Detection ..... Enabled
Remote AP Debug ..... Disabled
Logging trap severity level ..... informational
KPI not configured .....
Logging syslog facility ..... kern
S/W Version ..... 8.8.120.0
Boot Version ..... 1.1.2.4
[...]
Power Type/Mode..... PoE/Full Power
Number Of Slots..... 3
AP Model..... AIR-AP3802I-I-K9
AP Image..... AP3G3-K9W8-M
Cisco IOS Version..... 8.8.120.0
Reset Button..... Enabled
AP Serial Number..... FGL2114A4SU
[...]
```

Schurfdetectie kan op een AP worden ingeschakeld met deze opdracht:

```
(Cisco Controller) >config rogue detection enable ?
all          Applies the configuration to all connected APs.
<Cisco AP>  Enter the name of the Cisco AP.
```

Een lokale modus AP scant alleen landkanalen/DCA-kanalen en is afhankelijk van de configuratie. Als de schurk zich in een ander kanaal bevindt, kan de controller de schurk niet identificeren als u geen bewakingsmodus AP's in het netwerk hebt. Geef deze opdracht uit om te verifiëren:

```
(Cisco Controller) >show advanced 802.11a monitor

Default 802.11a AP monitoring
 802.11a Monitor Mode..... enable
 802.11a Monitor Mode for Mesh AP Backhaul..... disable
802.11a Monitor Channels..... Country channels
 802.11a RRM Neighbor Discover Type..... Transparent
 802.11a RRM Neighbor RSSI Normalization..... Enabled
 802.11a AP Coverage Interval..... 90 seconds
 802.11a AP Load Interval..... 60 seconds
 802.11a AP Monitor Measurement Interval..... 180 seconds
 802.11a AP Neighbor Timeout Factor..... 20
 802.11a AP Report Measurement Interval..... 180 seconds
```

- Rogue AP wordt niet uitgezonden via de SSID.
- Zorg ervoor dat het MAC-adres van de fraudebestendige AP niet wordt toegevoegd in de lijst van de minnelijke schurk of wordt vermeld via PI.
- De bakens van schurkenAP zijn niet bereikbaar aan AP die schurken ontdekte. Dit kan worden geverifieerd door de opname van de pakketten met een snuifje dicht bij de AP-

detector schurk.

- Een lokale modus van het toegangspunt kan tot 9 minuten duren voor er een bedrieglijke storing wordt gedetecteerd (3 cycli 180x3).
- Cisco AP's kunnen geen veelhoeken detecteren op frequenties zoals het publieke veiligheidskanaal (4,9 GHz).
- Cisco AP's kunnen geen schuren detecteren die aan FHSS (Frequency Hopping Spread Spectrum) werken.

Handige debugs

```
(Cisco Controller) >debug client
```

```
(If rogue mac is known)
```

```
(Cisco Controller) >debug client 50:2f:a8:a2:0a:60
```

```
(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP: 50:2f:a8:a2:0a:60 on slot 0
```

```
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -55, snr 39 wepMode 81 wpaMode 86, detectingIradTypes :20
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417.
Detecting Irad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel width (new/old :0/0) change detected on Detecting Irad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0 rssi -55, snr 39
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 IradInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule classification : Class malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mode = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0, ptype 318505456 mfp_supported 1
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 2

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly
```

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: butterfly

(Cisco Controller) >**debug dot11 rogue enable**

(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:

Debugging session started on Jun 05 08:39:46.828 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M09Y Hostname tiagoWLCcb

*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for processing Payload version:c1, slot:0 , Total Entries:5, num entries this packet:5 Entry index :0, pakLen:285

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTime-now)=152838

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src b0:72:bf:93:e0:d7 channel 1 rssi -59 ssid SMA1930072865

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src 50:2f:a8:a2:0a:60 channel 1 rssi -63 ssid butterfly

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src 00:a3:8e:db:01:a1 channel 13 rssi -16 ssid

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src a4:c3:f0:cf:db:18 channel 40 rssi -26 ssid blizzard

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -28, snr 61 wepMode 81 wpaMode 82, detectinglratypes :30

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src 00:a3:8e:db:01:b2 channel 40 rssi -28 ssid

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0 Detecting lrad: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: knownApCount=0, totalNumOfRogueEntries=5, #entriesThisPkt=5, #totalEntries=5

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -16, snr 76 wepMode 81 wpaMode 82, detectinglratypes :28

*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: avgNumOfRogues[0]/10=4, rogueAlarmInitiated[0]=0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 SYNC for Channel (new/old : 40/0) or channel width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0 Detecting lrad: 00:27:e3:36:4d:a0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 SYNC for Channel (new/old : 13/0) or channel width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0 rssi -28, snr 61

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0 rssi -16, snr 76

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 ReceiveSlotId = 0 ReceiveBandId = 1

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclassified, Change by Default State Alert Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xffff0617238

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for : Class Change by Default State Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Added Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP table

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either in AP list or neighbor, known or Mobility group AP lists

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclassified, Change by Default State Alert Change by Default

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200 for rogue AP b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue AP: 00:a3:8e:db:01:b2 autocontain = 2 Mode = 2

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0, ptype -155740480 mfp_supported 1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -59, snr 36 wpaMode 81 wpaMode 83, detectinglradtypes :20

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for : Class Change by Default State Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Send Rogue Info Notificaiton for AP report 00:27:e3:36:4d:a0 Rogue ssid change from to SMA1930072865

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecting lrad: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclassified, Change by Default State Alert Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -59, snr 36

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 RadioType: 3 lradInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue before Rule Classification : Class

unconfigured, Change by Default State Pending Change by Default

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue AP: 00:a3:8e:db:01:a1 autocontain = 2 Mode = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrاد, cannot apply rogue rule

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification : Class unconfigured, Change by Default State Pending Change by Default

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0, ptype -155740480 mfp_supported 1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel = 1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 6

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 1, apAuthEnabled on mac 0, ptype 318505456 mfp_supported 1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 2

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Found Rogue AP: 00:a3:8e:db:01:b0 on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg new Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -26, snr 61 wepMode 81 wpaMode 82, detectinglrادtypes :32

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecting lrاد: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -63, snr 5 wepMode 81 wpaMode 86, detectinglrادtypes :20

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 SYNC for Channel (new/old : 40/0) or channel width (new/old :0/0) change detected on Detecting lrاد: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecting lrاد: 00:27:e3:36:4d:a0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel width (new/old :0/0) change detected on Detecting lrاد: 00:27:e3:36:4d:a0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0 rssi -26, snr 61

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0 rssi -63, snr 5

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lrادInfo->containSlotId = 1 ReceiveSlotId = 0 ReceiveBandId = 1

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lrادInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 ssidLen = 8 min = 8 00:a3:8e:db:01:b0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 This rogue does not use my ssid. Rogue ssid=blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue AP: 00:a3:8e:db:01:b0 autocontain = 2 Mode = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=buterfly

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mode = 7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 2

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0, ptype 318505456 mfp_supported 1

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 2

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 New AP report 00:27:e3:36:4d:a0 rssi - 37, snr 50

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, snr 50

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, snr 43

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New AP report 00:27:e3:36:4d:a0 rssi - 62, snr 32

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, snr 32

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP table

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either in AP list or neighbor, known or Mobility group AP lists

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP:
b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg change state Rogue AP:
b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Deleting Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at
0xffff0617238

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg delete for Rogue AP:
b0:72:bf:93:e0:d7

Verwachte Trap-logbestanden

Zodra een schurk wordt gedetecteerd/verwijderd uit de schurkenlijst:

Wed jun 5 0 09:01:57 2019 Rogue-client: b4:c0:f5:2b:4f:90 wordt **gedetecteerd** door 1 APs schurken client-bundel:
a6:b1:e9:f0:e8:41, Staat: Waarschuwing, laatste detectie van AP:00:27:e3:36:4d:a0 Rogue
gateway mac 00:00:00:02:02:02.

Wed jun 5 1 09:00:39 2019 Rogue AP : 9c:97:26:61:d2:79 **verwijderd** van basisradio MAC : 00:27:e3:36:4d:a0-
interfacenr:0(802.11n(2,4 GHz))

Wed jun 5 2 08:53:39 2019 Rogue AP : 7c:b7:33:c0:51:14 **verwijderd** van basisradio MAC : 00:27:e3:36:4d:a0-
interfacenr:0(802.11n(2,4 GHz))

Wed jun 5 3 08:52:27 2019 Rogue-client: fc:3f:7c:5f:b1:1b wordt **gedetecteerd** door 1 APs-schurken clientlaag:
50:2f:a8:a2:0a:60, Staat: Waarschuwing, laatste detectie van AP:00:27:e3:36:4d:a0 Rogue
gateway mac 00:26:44:73:c5:1d.

Wed jun 5 4 08:52:17 2019 Rogue AP : d4:28:d5:da:e0:d4 **verwijderd** van basisradio MAC : 00:27:e3:36:4d:a0-
interfacenr:0(802.11n(2,4 GHz))

Aanbevelingen

1. Configureer de kanaalscan naar alle kanalen als u vermoedt dat er mogelijk fouten in uw netwerk zijn.
2. Het aantal en de locatie van bedrieglijke detectie AP's kan variëren van één per vloer tot één per gebouw en is afhankelijk van de lay-out van het bekabelde netwerk. Het is raadzaam om ten minste één schurkendetector AP in elke verdieping van een gebouw. Omdat een bedrieglijke detector AP een trunk vereist naar alle Layer 2 netwerk uitzendingsdomeinen die moeten worden bewaakt, is plaatsing afhankelijk van de logische lay-out van het netwerk.

Als de Rogue niet geclassificeerd is

Controleer of de schurkenregels goed zijn geconfigureerd.

Handige debugs

(Cisco Controller) >**debug dot11 rogue rule enable**

(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:

Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M09Y Hostname tiagoWLCcb

(Cisco Controller) >

*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154623, wep=1, ssid=blizzard slotId = 0 channel = 13 snr = 76 dot11physupport =

*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid= slotId = 0 channel = 13 snr = 77 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5790, wep=1, ssid=NOWO-A2121 slotId = 0 channel = 1 snr = 4 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5820, wep=1, ssid=NOWO-A2121 slotId = 0 channel = 1 snr = 4 dot11physupport = 3

*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154353, wep=1, ssid=buterfly slotId = 0 channel = 11 snr = 30 dot11physupport =

*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 **Rogue Classification:malicious, RuleName:TestRule, Rogue State:Containment Pending**

*apfRogueTask_3: Jun 05 09:13:27.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154713, wep=1, ssid= slotId = 0 channel = 13 snr = 77 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid=blizzard slotId = 0 channel = 13 snr = 76 dot11physupport =

*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRule, Rogue State:Containment Pending

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154743, wep=1, ssid= slotId = 0 channel = 13 snr = 77 dot11physupport = 3

Aanbevelingen

Als u bekende frauduleuze meldingen hebt, kunt u deze toevoegen in de gebruiksvriendelijke lijst of de validatie met AAA inschakelen en ervoor zorgen dat bekende cliëntmeldingen aanwezig zijn in de AAA-database (Verificatie, autorisatie en accounting).

RLDP identificeert geen Rogues

- Als de schurk zich in het DFS-kanaal bevindt, werkt RLDP niet.
- RLDP werkt alleen als het schurkenWLAN is geopend en DHCP beschikbaar is.
- Als het lokale toegangspunt de client in het DFS-kanaal bedient, neemt het niet deel aan het RLDP-proces.
- RLDP wordt niet ondersteund op AP-modellen 1800i, 1810 EAP, 1810W, 1815, 1830, 1850, 2800 en 3800 Series AP's.

Handige debugs

(Cisco Controller) >debug dot11 rldp enable

!--- RLDP not available when AP used to contain only has invalid channel for the AP country code

*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 **Invalid channel 1 for the country IL for AP
00:27:e3:36:4d:a0**
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request

!--- ROGUE detected on DFS channel

*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e **Our AP 00:27:e3:36:4d:a0 detected this rogue on
a DFS Channel 100**
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request

!--- RLDP is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Received request to detect Rogue
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a **Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model:
AIR-AP1852I-E-K9**
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue *apfRLDP: Jun
05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad *apfRLDP: Jun 05 15:02:49.602:
50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9 *apfRLDP: Jun
05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0 *apfRLDP: Jun 05 15:02:49.602:
50:2f:a8:a2:0a:61 **Monitor Mode AP found b4:de:31:a4:e0:30 with RSSI -61**
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 found closest monitor AP b4:de:31:a4:e0:30 slot
= 0, channel = 1

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Found RAD: 0xffd682b5b8, slotId = 0, Type=1
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 AP b4:de:31:a4:e0:30 Client b4:de:31:a4:e0:31
Slot = 0
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 WARNING!!!! mscb already exists!

*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central
switched to TRUE
*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61 **rldp started association, attempt 1**
*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time.
RLDP State(2)

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time.
RLDP State(2)

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3
*apfOpenDtlSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.
*apfOpenDtlSocket: Jun 05 15:03:00.808: **50:2f:a8:a2:0a:61 RLDP state RLDP_ASSOC_DONE (3).**

```
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Successfully associated with rogue:  
50:2F:A8:A2:0A:61  
  
!--- Attempt to get ip from ROGUE  
  
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Starting dhcp  
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue  
50:2f:a8:a2:0a:61  
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST  
  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 htype: Ethernet  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hlen: 6  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hops: 1  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 xid: 0x3da1f13  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 secs: 0  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 flags: 0x0  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 hw_addr: B4:DE:31:A4:E0:31  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 client IP: 0.0.0.0  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 my IP: 0.0.0.0  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 server IP: 0.0.0.0  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 gateway IP: 0.0.0.0  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 options:  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 DHCP message: 1 DISCOVER  
*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)  
*apfRLDP: Jun 05 15:03:00.870: [0000] 02 40  
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 host name: RLDP  
  
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP  
50:2f:a8:a2:0a:61  
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61  
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue  
50:2f:a8:a2:0a:61  
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST  
  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 htype: Ethernet  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 hlen: 6  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 hops: 1  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 xid: 0x3da1f13  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 secs: 0  
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 flags: 0x0
```

```
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31 server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31 gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31 options:
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31 DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)
*apfRLDP: Jun 05 15:03:10.878: [0000] 02 40
*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31 host name: RLDP
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 htype: Ethernet
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 hlen: 6
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 hops: 1
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 xid: 0x3da1f13
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 secs: 0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 flags: 0x0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 hw_addr: B4:DE:31:A4:E0:31
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 client IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 my IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 server IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 gateway IP: 0.0.0.0
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 options:
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 DHCP message: 1 DISCOVER
*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)
*apfRLDP: Jun 05 15:03:20.885: [0000] 02 40
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 host name: RLDP
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP
50:2f:a8:a2:0a:61
```

!--- RLDP DHCP fails as there is no DHCP server providing IP address

```
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCP FAILED state for rogue
50:2f:a8:a2:0a:61 *apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 DHCP failed *apfRLDP: Jun 05
15:03:20.885: Waiting for ARLDP request
```

Aanbevelingen

1. Start RLDP handmatig op verdachte bedrieglijke meldingen.
2. Plan RLDP periodiek.
3. RLDP kan worden geïmplementeerd op lokale toegangspunten of toegangspunten met monitormodus. Voor de meeste schaalbare implementaties en om elke invloed op de clientservice te elimineren, moet RLDP indien mogelijk worden geïmplementeerd op AP's in de monitormodus. Deze aanbeveling vereist echter dat een AP-overlay voor monitormodus wordt geïmplementeerd met een typische verhouding als 1 AP voor elke 5 AP met lokale modus. AP's in de Adaptieve IPS-monitormodus kunnen ook voor deze taak worden gebruikt.

Schurfdetectie - AP

Schurkentoegang in een schurkendetector kan worden gezien met deze opdracht in de AP-console. Voor bekabelde hengsten verplaatst de vlag zich om de status in te stellen.

```
tiagoAP.6d09.fff0#show capwap rm rogue detector
LWAPP Rogue Detector Mode
Current Rogue Table:
Rogue hindex = 0: MAC 502f.a8a2.0a61, flag = 0, unusedCount = 1
Rogue hindex = 0: MAC 502f.a8a2.0a60, flag = 0, unusedCount = 1
Rogue hindex = 7: MAC 502f.a8a2.0d41, flag = 0, unusedCount = 1
Rogue hindex = 7: MAC 502f.a8a2.0d40, flag = 0, unusedCount = 1
```

```
!--- once rogue is detected on wire, the flag is set to 1
```

Handige debug-opdrachten in een AP-console

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dc0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3fff0
```

*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.alcc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.alcc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.alcc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.alcc.0e9e

Schurkenbeperring

Verwachte debugs

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Updated AP report b4:de:31:a4:e0:30 rssi -33, snr 59
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Looking for Rogue 00:a3:8e:db:01:b0 in known AP table
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP 00:a3:8e:db:01:b0 is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6
ContainmentLevel : 4 level 4

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected by AP: b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RadioType: 2 lradInfo->containSlotId = 1
ReceiveSlotId = 1 ReceiveBandId = 1

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue before Rule Classification : **Class malicious, Change by Auto State Contained Change by Auto**

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule classification : Class malicious, Change by Auto State Contained Change by Auto

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 **Rogue AP: 00:a3:8e:db:01:b0 autocontain = 1 Mode = 6**

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 apfRogueMode : 6
apfRogueContainmentLevel : 4 lineNumber : 8225 apfRogueManualContained : 0 function :
apfUpdateRogueContainmentState

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0
contains slot 1 for detecting lrad 00:27:e3:36:4d:a0.
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0
RSSI = -28
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0
RSSI = -31
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30
RSSI = -33
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -28 totClientsDetected = 2

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI
= -31 totClientsDetected = 2
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI
= -33 totClientsDetected = 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP
00:27:e3:36:4d:a0. Containment mode 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP
00:27:e3:36:4d:a0. Containment mode 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP
b4:de:31:a4:e0:30. Containment mode 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Contains rogue with 3 container
AP(s).Requested containment level : 4
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Checking Impersonation source
00:a3:8e:db:01:b0 detected by b4:de:31:a4:e0:30, FailCnt 0, mode 6, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0
mfp Impersonation 0 ids flags 3
```

Aanbevelingen

1. Het toegangspunt met lokale/Flex-verbodingsmodus kan 3 apparaten per radio tegelijk bevatten en het toegangspunt met monitormodus kan 6 apparaten per radio bevatten. Zorg er bijgevolg voor dat het toegangspunt niet het maximale aantal toegestane apparaten bevat. In dit scenario is de client in een inperking hangende status.
2. Controleer de regels voor automatische insluiting.

Conclusie

Schurfdetectie en -beperking in de gecentraliseerde Cisco-controlleroplossing is de meest effectieve en minst ingrijpende methode in de sector. De flexibiliteit die aan de netwerkbeheerder wordt geboden, maakt een meer aangepaste pasvorm mogelijk die aan alle netwerkvereisten kan voldoen.

Gerelateerde informatie

- [Configuratiehandleiding voor Cisco draadloze controllers, release 8.8 - Beheer van rackservers](#)
- [Beste praktijken voor configuratie van Cisco draadloze LAN-controllers \(WLC\)](#)
- [Implementatiegids voor WLC 3504 release 8.5](#)
- [Implementatiehandleiding voor Cisco 5520 draadloze LAN-controllers](#)
- [Releaseopmerkingen voor Cisco draadloze controllers en lichtgewicht access points, Cisco draadloze release 8.8.120.0](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.