

# اهم في فختل او عاطل ا فاشتكا تالكشم لح ةدحوم ةيكلسال ةكبش يف

## تاي وتحمل

[قمدقملا](#)

[قيس اس الاب طتملا](#)

[تابلطتملا](#)

[قمدختسملا باتانوكملما](#)

[نديع داخلملا ايلع قمعاع قرطن](#)

[عداخلملا فاشتكا](#)

[قاتقلاب جراخ صحف](#)

[قبقراهملا عرض و صحف](#)

[قشاشلا عرض و ميلحملاب عرض ولا نيب قبراقم](#)

[عداخلملا ايلع فرعتلما](#)

[فقرام تاليجست](#)

[قعداخلملا ليصافتلما](#)

[قدراهملا ثادحلاب ريدصتلما](#)

[قلبي خدلاب الجسلابا قلهم عاهتنا](#)

[عداخلملا فشاللاب عرض ولا ظقطن](#)

[قعي سوتلما قيلباق تارابتععا](#)

[RLDP](#)

[تابطفتح RLDP](#)

[لو حملما ذفننم تاراسم](#)

[نديقراهملا فينصت](#)

[نديقراهملا فينصت دعائق](#)

[قىداقيق HA](#)

[تدملابلا اصاصتالا قىداقيق](#)

[قعداخلملا رطاخلملا في فخت](#)

[نديع داخلملا عاونتحا](#)

[قعداخلملا عاونحالاب ليصافت](#)

[يىقاوللت عاونتحا](#)

[قرام عاونتحا](#)

[لو حملما دفنم ليغشت فاقيرما](#)

[نديوكتلما](#)

[عاطلابانع فشكلا نديوكت](#)

[عداخلملا فاشتكا قاتقلل يىوض لاحس اهملا نديوكت](#)

[عداخلملا فينصت نديوكت](#)

[عاطلابا في فخت نديوكت](#)

[يوديلابا عاونحالابا نديوكت](#)

[يىقاوللت عاونتحا](#)

[ل قيس اس الاب ئينبل اعم Prime](#)

[تحصلابا تم ققحتلما](#)

[اهحالص او عاطلابا فاشتكتسا](#)

[دغولابا فاشتكا متى مل اذا](#)

[قدی فمل ا عاطخألا حیحصت](#)

[عوقوتمل ا قمیالمل ا تالجس](#)

[تایصوت](#)

[فنن صم دیغ دغول، ناک اذا](#)

[قدی فمل ا عاطخألا حیحصت](#)

[تایصوت](#)

[داغوألا عقة و م درجي ال RLDP](#)

[قدی فمل ا عاطخألا حیحصت](#)

[تایصوت](#)

[عداخمل ا فش اکل لوص ول ا ظقون](#)

[لوص ول ا ظقون مکحت درجوي ف قدی فمل ا عاطخألا حیحصت رماوا](#)

[نیعداخمل ا عاوتحا](#)

[عوقوتمل ا عاطخألا حیحصت](#)

[تایصوت](#)

[رارقلل ا](#)

[قلص تاذ تامولعم](#)

---

## ةمدملا

ةيكللسالل Cisco تاکب بش ىلع اهراث آن م في فختل او عاطخألا فشك ٰ قي ثوا ذه فصي.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلاتل ا عيضاوملاب ٰ فرع م كيدل نوكت نأب Cisco يصوت:

- نم ٰ كبسالل LAN ٰ كبس يف مکحتل ا تادحو Cisco.
- ل ٰ ساسألا ٰ نبلا Cisco Prime.

### ةمدختسملا تانوكمل

ةيلاتل ا ٰ دامل ا تانوكمل او جماربل ا تارادص ا ىل ا دنتسملا اذه يف ٰ دراول ا تامولعملا دنتست:

- لسالسل Cisco نم ٰ دحومل ا ٰ كبسالل LAN (LAN) ٰ كبس شل ا يف مکحتل ا تادحو 8.8.120.0 رادص إل ا لغشت يتل ا 3504 و 8540 و 5520.

- 3802 و 2802 و 1832 و 1852 نم لوصول ا طاقن.

- 1. ٰ جومل ا نم 1700 و 2700 و 3700 نم لوصول ا طاقن.

صاخ ٰ يل معم ٰ يب يف ٰ دوجومل ا ٰ زهجألا نم دنتسملا اذه يف ٰ دراول ا تامولعملا عاشن ا مت تناك اذا . (يضا رتفا) حوس مم نيك تب دنتسملا اذه يف ٰ مدختسملا ٰ زهجألا عيمج تأدب رمأ يأ ل متحمل ا ريثأت ل ل كمه ف نم دكأ تف ، ليغشت ل ا ديق كت كبس.

## نیعداخمل ا ىلع ٰ ماع ٰ رظن

لوصول او نیلماعل ا ٰ يجاتن ا نم ديزتو ٰ يكللس ل ا تاکب بش ل ا تاکب بش ل ا عسوت

نم ۆي باض ١ ۆقبط اه ب حرص ملا ریغ ۆي کلساللا ۆكبشلا لى ثمت، كلذ عم و. تامولعملالا ىلا دعٽ، ۆي کلسالا تاكبشلا ىلع ذفنملا نامأ يف ريكفتلا ليلىقت عم. ۆينمألا فواخملالا يذلا فظوملا نإف، ييلاتلابو. ۆي کلسالا تاكبشلل الھس ادادتما ۆي کلساللا تاكبشلا وأ ۆي کلسال ۆيساسأ ۆينب ىلا Cisco ریغ وأ (Cisco) ھب ۆصالخالا لوصولالا ۆطقن رضحى ھذه ىلا لوصولاب مھل حرص ملا ریغ نيم دخت سملل حمسىو ديج لكش ب ۆنم ۇرم ۆي کلس ۆنما ۆكبش قارتىخا ۆلۋەس ب ھنكىمىي، رخآل لكش ب ۆنم ۇرم تناناڭ يىتللا ۆكبشلا.

اهيلع عاضقول او هذه نامألا ةلكلش م ةبقارم ئيناكما ةكبشلا لوطسمل عداخمل ا فشكلا حيتي  
الملماك الـح حيـتـتـ يـتـلـا عـداخـمـلـا فـشـكـلـلـ اـقـرـطـ Cisco نـمـ ةـدـحـوـمـلـا ةـكـبـشـلـا ةـيـنـبـ رـفـوتـ  
بعـصـيـ ةـفـلـكـمـ ةـيـشـغـتـ تـاـوـدـأـوـنـاـكـبـشـ يـلـا ةـجـاحـلـا نـوـدـ نـيـعـداخـمـلـا ءـاوـتـحـالـاـوـ فـيـرـعـتـلـلـ  
اهـرـيـرـبـتـ.

دغولا حبصيو .ع داخم هنأ ىلع كلبق نم ھترادا مرت الو كفيط كراشي زاهج يأ رابتع نكمي  
تاهوي رانيسلا ھذه لثمم يف اري طخ

- (لسع ۋەدعاق) كىتكىبىش لىثم (SSID) ۋەمىخلا ۋە وەجم فرعەم سەفن مادختىسىل دادعىلدا دىنۇ
  - ئېكلىسلىا ۋە كىبىشلىا ىلىع ھفاشتىكا دىنۇ
  - ئەصصەم سەئارە
  - ئەثىپ بىخ ئېنېب، نايچەلە مۆظۈم يىف، جراخىلا نەم صىخش لىبق نەم ھدادعى دىنۇ

رطاخملانم دحىندأىلارىقىتلىنىقىراملا نع فشكلا مادختسى يە تاسرامملالىصفأو تاڭرىشلا ۋەئىب يېف، ئالثىم، ۋەئىنمألا.

لیبس یلع ،عداخملالا نع فشكلا یلإ اهیف جاتحت ال ةنیعم تاهویرانیس کانه ،کلذ عمونکامألا یفو ۋەنیدملاءاحنأ عیمچ یفو Office Extend Access Point (OEAP) رشن یف ،لاثملالا ۋەجراخلا.

مدقي نل نيعداخملانع فشكـلـل ئـيجـراـخـلا ئـيتـوبـكـنـعـلـا ئـكـبـشـلـا لـوـصـوـ طـاقـنـ مـادـخـتـسـاـ نـاـ  
لـيلـحـتـلـل درـاوـمـلـا مدـخـتـسـي فـوسـ هـنـأـ نـيـحـ يـفـ ئـرـبـكـ ئـمـيقـ.

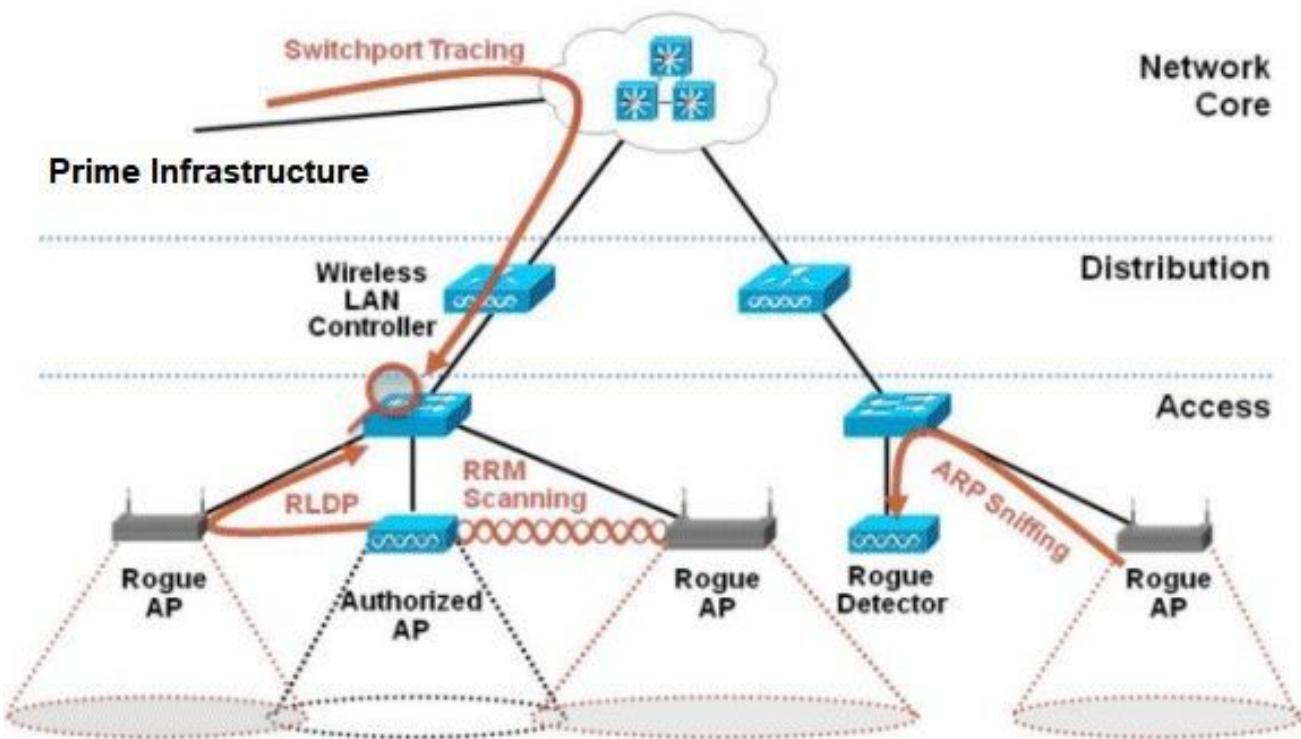
كـانـهـ نـأـلـ ، (لمـاـكـلـابـ مشـتـحـمـلاـ يـئـاقـلـتـلـاـ عـاوـتـحـالـاـ بـنـجـتـ وـأـ)ـ مـيـيقـتـ نـاـكـمـبـ ئـيـمـهـأـلـاـ نـمـ ، اـرـيـخـأـوـ .ـيـئـاقـلـتـ لـكـشـبـ لـمـعـلـلـ تـكـرـتـ اـذـاـ قـلـمـتـحـمـ ئـيـنـوـنـاـقـ تـايـلـوـفـسـمـ وـ ئـيـنـوـنـاـقـ اـيـاضـقـ

UWN) ةدحوملا ةيكلساللا ةكبشلا لجيف ةعداـملـا ةـزـهـجـأـلـا ةـرـادـإـلـ ةـيـسـيـئـرـ لـجـارـمـ ثـالـثـ كـانـهـ Cisco:

- ڦڙهجأ دوجو فاشتكال (RRM) ڦيكلساللا دراوملا ڦارادا صحف مادختسا متى - فشكلا ڻاخم.
  - فاشتكا ڦڙهجأو، (RLDP) راودلا عقوملا فاشتكا لوكوتورب مادختسا متى - فينصتلما ناك اذا ام ديدحتل لوحملما ذفانم عباوت و (طقف 1 ڦجوملا نم (AP) لوصولما طاقن) لجدلا يف نيقراملا فينصت دعاوق دعاست امك. ڦيكلسلا ڦكبشلاب الصلتم يل اي خدلما زاهجلما هصئاصخ ىلا ادانتسا ڏدھم تائيٰ ىلا نيقراملا حيشرت.
  - بقعتل راودلا ءاوتحالا او راودلا عقوملا او لوحملما ذفانم قالغإ مادختسا متى - فيفتحتلما لاجدلما زاهجلما ديدهت لاطباو یل عفلما هعقوم.

# Cisco Rogue Management Diagram

## Multiple Methods



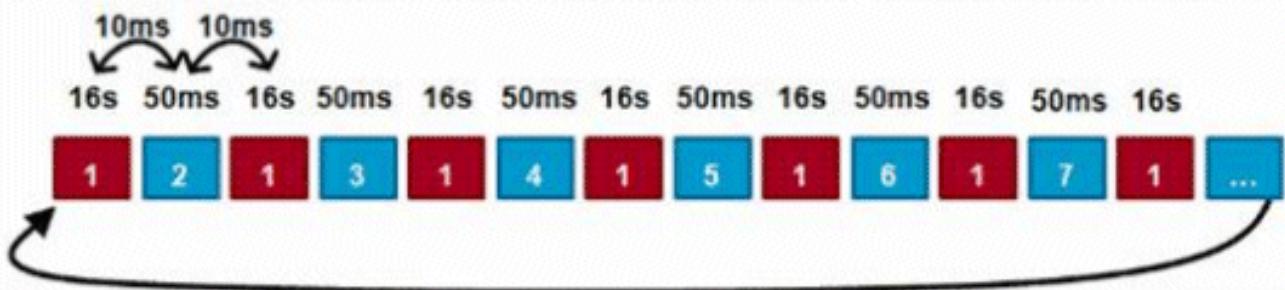
## عِدَّا خَمْلَا فَاشْتَكَ

طاقين كل ذنم ضت يو . كترطي س تحت سيل هنكل ، كفيط كراشي زاهج يأ و ه اس اسأ ع داخملها  
وع داخملها نارق ألا تاكب شو نيع داخملها ئا عالملا او ئيكلس الالا تاهجوملما او ئليخ دلا لوصولا  
Wi-Fi كبس هيلإ ئادنتسملا ئاع داخملها ئزههج ألا فاشتكال قرطلانم ادعع Cisco نم UWN مدخلتسى  
مادختسإ نكمي امك . ئاصص خملها ئشاشلا عض و تاناكم او ئانقلالا جراخ يئوضلها حسملالا لثم  
Cisco Spectrum Expert 802.11 لوكوتورب هيلإ دنتسىت ال يتلا ئاع داخملها ئزههج ألا ديدحتل  
Bluetooth روسج Bluetoth.

ةانقل ا جراخ صحف

يـ(ف) Flex-Connect ويلـحملـا عـضـولـا يـفـ لـوصـولـا طـاقـونـ طـاسـاوـبـ ئـيلـمعـلـا هـذـهـ ذـيـفـنـتـ مـتـيـ ئـانـقـلـا صـحـفـوـلـيـمـعـلـا قـمـدـخـ حـيـتـتـ يـتـلـا تـقـولـا مـيـسـقـتـ ئـيـنـقـتـ مـدـخـتـسـتـوـ (لـصـتـمـلـا عـضـولـا، ئـيـنـاثـ 16 لـكـ ئـيـنـاثـ يـلـلـمـ 50 ئـدـمـلـ ئـانـقـلـا جـرـاخـ لـلـا لـاـقـتـنـالـا عـمـ. ويـدارـلـا سـفـنـ مـادـخـتـسـابـ ئـمـدـخـ مـدـعـلـ اـهـتـقـوـنـمـ طـقـفـ ئـرـيـغـصـ ئـبـسـنـ يـضـارـتـفـاـلـ كـشـبـ قـفـنـتـ لـوصـولـا ئـطـقـنـ نـإـفـ لـصـافـلـا يـفـ. ثـدـحـتـ ئـيـنـاثـ يـلـلـمـ 10 ئـانـقـ رـيـيـغـتـ ئـرـتـفـ كـانـهـ نـأـضـيـأـ ظـحـالـ. عـالـمـعـلـا (1-11) FCC زـتـرـيـهـاجـيـجـ 2.4 ئـانـقـ لـكـ حـسـمـ مـتـيـ، ئـيـنـاثـ 180 نـمـ يـئـوضـلـا حـسـمـلـلـ يـضـارـتـفـالـ ئـطـقـنـ نـوـكـتـ، ETSI لـثـمـ، ئـرـخـأـلـا ئـيـمـيـظـنـتـلـا تـالـاـجـمـلـلـ ئـبـسـنـلـاـبـ. لـقـأـلـا لـلـعـ ئـدـحـاوـ ئـرـمـ يـئـوضـ ئـمـيـاـقـ نـمـ لـكـ طـبـضـ نـكـمـيـ. تـقـولـا نـمـ الـيـلـقـ لـلـعـأـ ئـيـوـئـمـ ئـبـسـنـلـ ئـانـقـلـا جـرـاخـ لـوصـولـا دـحـ بـعـادـأـلـا رـيـثـأـتـ دـيـدـحـتـ لـلـاـ يـدـوـيـ اـذـهـوـ. RRM نـيـوـكـتـ يـفـ يـئـوضـلـا حـسـمـلـا ئـرـتـفـوـ تـاـوـنـقـلـا اـمـدـنـعـ اـتـقـفـمـ صـحـفـلـا فـاقـيـإـلـا ئـيـمـزـراـوـخـلـا يـفـ ئـاـكـذـلـا ئـزـيـمـ نـيـمـضـتـ مـتـيـ اـمـكـ، 1.5%، ئـصـقـأـ تـوـصـلـا لـثـمـ، ئـيـلـاعـلـا ئـيـوـلـوـلـاـتـاـذـ ئـمـدـخـلـاـ ئـدـوـجـ تـارـاطـاـ مـيـلـسـتـلـ ئـجـاحـ كـانـهـ نـوـكـتـ

## Local-Mode AP on Channel 1 - 802.11 b/g/n Off-Channel Scanning

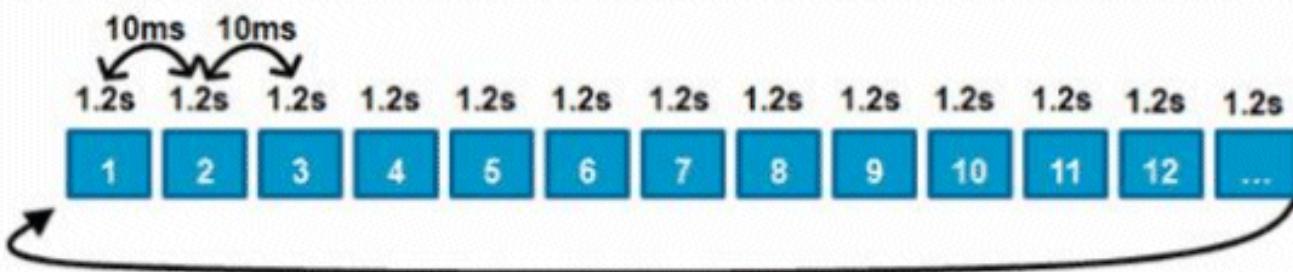


عوضولاييف لوصولا ةطقنل ةانقلاج راخ يئوضولاح سملاظيمزراوخل فصوصووه مسرلا اذه ويدارلا زاهج ىلع يزاوتلاب ٖلثامم ةيلمع مهتتو. زترىهاجيچ 2.4 تاجوملا ىدم يف يلحملاتقولا لثممي رمحأ عبرم لك. دح او روضح لوصولا ةطقن ىدلناك اذا زترىهاجيچ 5 درتب ىلع فورصملا تقولا لثممي قرزا عبرم لك امنيبي، ةيسيرللا APs ةانق ىلع فورصملا جسملا ضارغلأا ٖرواجملاتاونقلالا.

### ةبقارملالا عضوصحف

اده ةشاشللا عضوييف لوصولاطاقن ةطساوب ةيلمعلا هذه ذيفنت متي WIPS Monitor Mode APs يف تاونقلالا عيمج حسملا ويدارلا تقو نم 100% مدخلتسن يتلا ةانقل لك ىلع ربكاً تقو عاصق حيتى وربكاً فاشتكا ئعرس حيتى اذهو. صاخ يددرت قاطن ئالمعلا فاشتكا ىلع ئوقوفتم اضيأ ةبقارملالا عضوييف لوصولاطاقن نوكت. ةيدرف ةانقل لك يف ثدحي يذلا طاشنلل الومش رثكاً ضرع ئقيرط مهيدلنا ثيحن يع داخملالا.

## Monitor-Mode AP - 802.11b/g/n Scanning All Channels



زاهج عضوييف لوصولاطقنل ةانقلاج راخ يئوضولاح سملاظيمزراوخل فصوصووه مسرلا اذه درتب ويدارلا زاهج ىلع يزاوتلاب ٖلثامم ةيلمع مهتتو. زترىهاجيچ 2.4 تاجوملا ىدم يف ضرعلا دح او روضح لوصولاطقن ىدلناك اذا زترىهاجيچ 5.

### ةشاشللا عضوويلحملالا عضولالا نيب ئنراقم

اًشح بتاونقلالا حسم و WLAN عالمع ئمدخ نيب اهتارود يلحملالا عضولل لوصولاطقنم مسقت ناروديلل لوطاً اتقو يلحملالا عضولالا يف لوصولاطقنق رغتسن، كلذل ٖوجيتن. تاديدهتلانع ال ىتح ئنيعم ةانق يأ ىلع عيمجتلاتاناييب يف لقاً اتقو قفتامك، تاونقلالا عيمج رباع 3 نم) لوطاً تاراجشلارو تامجهلا دصرتاقوا نوكت، كلذل ٖوجيتنو. ليملعلا تايملمع ليطعت متي عم ئنراقم ئاوهلاربع مهت يتلا تامجهلا نم رغصأ قاطن فاشتكا نكمي و (ٖقىقد 60 ىلإ

## ةشاشلا عضويه لوصولا ةطقن.

اديدجت لقاً، نيعداخملاءالعالمعـلـا لـثـمـ، ةـعـطـقـتـمـلـا رـوـرـمـلـا ةـكـرـحـ نـعـ فـشـكـلـا نـإـفـ، كـلـذـىـلـعـ ةـوـالـعـ هيـفـ مـتـيـ يـذـلـا تـقـوـلـا سـفـنـ يـفـ روـرـمـلـا ةـكـرـحـ ةـانـقـ ئـلـعـ نـوـكـتـ نـأـ بـجـيـ (AP) لـوـصـوـلـا ةـطـقـنـ نـأـلـ لـوـصـوـلـا ةـطـقـنـ يـضـقـتـ . تـالـاـمـتـحـاـلـا ئـلـعـ اـنـيـرـمـتـ اـذـهـ حـبـصـيـ . اـهـلـاـبـقـتـسـاـ وـأـ روـرـمـلـا ةـكـرـحـ لـاـسـراـ يـتـلـاـ تـامـجـهـلـاـوـ نـيـعـداـخـمـلـاـ نـعـ ثـحـبـلـلـ تـاـونـقـلـاـ حـسـمـ ئـلـعـ اـهـتـارـوـدـعـيـمـجـ ةـشـاشـلـاـ عـضـوـبـ ةـصـاخـلـاـ تـقـوـلـاـ سـفـنـ يـفـ ضـرـعـلـاـ زـاهـجـ عـضـوـبـ ةـصـاخـلـاـ لـوـصـوـلـاـ ةـطـقـنـ مـادـخـتـسـاـ نـكـمـيـ . عـاـوـهـلـاـ رـبـعـ مـتـ زـاهـجـ عـضـوـتـامـدـخـوـ (ـقـايـسـلـاـ ةـاعـارـمـعـ)ـ عـقـوـمـلـاـوـ فـيـكـتـلـلـ لـبـاـقـلـاـ ضـرـعـلـاـ زـاهـجـ عـضـوـتـامـدـخـلـاـ ئـرـخـأـلـاـ ضـرـعـلـاـ.

امـدنـعـ . فـشـكـلـلـ تـقـوـلـقـأـ دـيـاـوـفـلـاـ نـوـكـتـ ، ةـبـقـارـمـلـاـ عـضـوـيـفـ لـوـصـوـلـاـ طـاقـنـ رـشـنـ مـتـيـ اـمـدنـعـ عـنـمـ مـاـظـنـ مـادـخـتـسـابـ يـفـاـضـاـ لـكـشـبـ ةـبـقـارـمـلـاـ عـضـوـيـفـ لـوـصـوـلـاـ طـاقـنـ نـيـوـكـتـ مـتـيـ ربـعـ تـامـجـهـلـاـوـ تـادـيـدـهـتـلـاـ نـمـ عـسـوـأـ قـاطـنـ فـاـشـتـكـاـ نـكـمـيـ ، فـيـكـتـلـلـ لـبـاـقـلـاـ (WIPS)ـ تـاقـاـرـتـخـاـلـاـ عـاـوـهـلـاـ.

يلـحـمـلـاـ عـضـوـلـاـ ئـلـاـ لـوـصـوـلـاـ طـاقـنـ	ضرـعـلـاـ زـاهـجـ عـضـوـلـاـ لـوـصـوـلـاـ طـاقـنـ
تقـوـلـاـ مـيـسـقـتـ ةـزـيمـ لـالـخـ نـمـ عـالـمـعـلـاـ مـدـخـيـ ةـانـقـلـاـ جـرـاـخـ يـئـوـضـلـاـ حـسـمـلـاـبـ	صـصـخـمـ يـئـوـضـ حـسـمـ
ئـلـعـ ةـيـنـاثـ يـلـلـمـ 50ـ ئـلـاـ عـاـمـتـسـاـلـاـ نـآـلـاـ مـتـيـ ةـانـقـ لـكـ	ةـانـقـ لـكـ ئـلـعـ 1.2sـ لـ عـمـتـسـيـ
حـسـمـلـلـ ةـئـيـهـتـلـلـ لـبـاـقـ : • تـاـونـقـلـاـ ةـفـاـكـ • (ـيـضـاـرـتـفـاـلـاـ)ـ دـلـبـلـاـ تـاـونـقـ • DCAـ تـاـونـقـ	تـاـونـقـلـاـ لـكـ حـسـمـ

## عـداـخـمـلـاـ ئـلـعـ فـرـعـتـلـاـ

لـوـصـوـ طـاقـنـ لـبـقـ نـمـ عـداـخـمـ زـاهـجـ نـمـ دـاـشـرـاـلـاـ ةـزـهـجـأـ وـأـ رـاـبـسـمـلـاـ ةـبـاـجـتـسـاـ ئـلـاـ عـاـمـتـسـاـلـاـ مـتـ اـذـاـ ربـعـ تـامـوـلـعـمـلـاـ هـذـهـ لـيـصـوـتـ مـتـيـ ذـئـنـيـحـ ، ةـبـقـارـمـلـاـ عـضـوـيـفـ وـأـ نـرـمـ لـاـصـتـاـ تـاـذـ وـأـ ةـيـلـحـمـ (APs)ـ عـنـمـلـ . ةـيـلـمـعـلـلـ (WLC)ـ ةـيـكـلـسـاـلـلـاـ ةـيـلـحـمـلـاـ ةـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ ةـدـحـوـ ئـلـاـ CAPWAPـ ئـرـخـأـلـاـ لـوـصـوـلـاـ طـاقـنـ فـيـرـعـتـ مـدـعـ نـاـمـضـلـ قـرـطـلـاـ نـمـ دـدـعـ مـادـخـتـسـاـ مـتـيـ ، ةـئـطـاخـلـاـ تـايـبـاجـيـاـلـاـ ـقـعـوـمـجـ تـاثـيـدـجـتـ قـرـطـلـاـ هـذـهـ نـمـضـتـتـوـ . عـداـخـمـ زـاهـجـ اـهـنـأـ ئـلـعـ Ciscoـ ئـلـإـ ةـدـنـتـسـمـلـاـ ةـرـادـمـلـاـ ةـيـنـبـلـاـ رـبـعـ اـهـبـ حـوـمـسـمـلـاـ ةـمـئـاـقـلـلـ ةـفـوـلـأـمـلـاـ (AP)ـ لـوـصـوـلـاـ طـاقـنـ وـوـرـاـجـمـلـاـ RFـ مـزـحـوـ لـقـنـتـلـاـ لـ ةـيـسـاسـأـلـاـ ةـيـسـاسـأـلـاـ ةـيـسـاسـأـلـاـ Primeـ (PI).

## ةـقـرـامـ تـالـيـجـسـتـ

ةـعـوـمـجـمـلـاـ ئـلـعـ طـقـفـ يـوـتـحـتـ مـكـحـتـلـاـ ةـدـحـوـبـ ةـصـاخـلـاـ رـاـوـدـلـاـ زـاهـجـلـاـ تـاـنـاـيـبـ ةـدـعـاـقـ نـأـ نـيـحـ يـفـ مـلـ لـجـسـ تـاـغـوـارـمـ وـثـدـحـ لـجـسـ اـضـيـأـ نـمـضـتـتـ piـ نـإـفـ ، اـهـفـاـشـتـكـاـ مـتـ يـتـلـاـ عـداـخـمـلـاـ نـمـ ةـيـلـاحـلـاـ

ةيئرم دعت.

## ةعداً خالل لوصول افـتـالـا

ىـلـا عـامـتـسـالـل ةـيـنـاثـ يـلـلـمـ 50 ةـدـمـلـ ةـانـقـلـا جـرـاخـ لـاقـتـنـالـابـ CAPWAPـ لـوـصـوـلـا ةـطـقـنـ مـوقـتـ وـأـعـالـمـ يـأـ لـاسـراـ مـتـيـ . تـاـونـقـلـا لـخـادـتـ وـعـاصـوـضـلـا نـعـ اـثـحـبـ ةـبـقـارـمـلـا وـنـيـعـداـخـمـلـا ءـالـمـعـلـا ةـيـلـاتـلـا تـاـمـوـلـعـمـلـا عـمـجـتـ يـتـلـاـوـ ، مـكـحـتـلـاـ وـدـحـوـلـاـ مـهـفـاشـتـكـاـ مـتـ نـيـعـداـخـمـ (APـ) لـوـصـوـ طـاـقـنـ:

- ةـعـداـخـمـلـا لـوـصـوـلـا ةـطـقـنـلـ MACـ نـاـوـنـعـ
- قـرـامـ صـخـشـكـ اـهـنـعـ فـشـكـلـا مـتـ يـتـلـا لـوـصـوـلـا ةـطـقـنـ مـسـاـ
- عـداـخـمـلـا لـصـتـمـلـا (ءـالـمـعـلـا) لـيـمـعـلـابـ صـاـخـلـا MACـ نـاـوـنـعـ
- ةـيـنـمـأـ ةـسـاـيـسـ
- ةـجـاـبـيـدـلـاـ
- ةـاعـضـوـضـلـاـ ئـلـاـ ةـرـاشـإـلـاـ ةـبـسـنـ (SNRـ)
- (RSSIـ) لـبـقـتـسـمـلـا ةـرـاشـإـاـ ةـوـقـ رـشـفـمـ
- لـجـدـلـاـ فـشـكـ ةـانـقـ
- قـرـامـ دـوـجـوـنـعـ فـشـكـلـا هـيـفـ مـتـيـ يـذـلـاـ وـيـدارـلـاـ
- عـداـخـمـلـا SSIDـ ثـبـ ةـلـاحـ يـفـ) عـداـخـمـلـاـ
- عـداـخـمـلـا IPـ نـاـوـنـعـ
- دـغـوـلـاـ نـعـ غـالـبـإـلـاـ مـتـيـ ةـرـمـ رـخـآـوـ لـوـأـ
- ةـانـقـلـاـ ضـرـعـ

## ةـقـرـامـلـاـ ثـادـحـأـلـاـ رـيـدـصـتـلـ

حـمـسـتـ ، ةـفـشـرـأـلـلـ (NMSـ) ةـيـجـرـاخـ ةـهـجـ ةـكـبـشـ ةـرـادـاـ مـاـظـنـ ئـلـاـ ةـعـداـخـمـلـاـ ثـادـحـأـلـاـ رـيـدـصـتـ لـجـأـ نـمـ ةـدـيـصـمـ تـالـبـقـتـسـمـ ةـفـاضـإـبـ (WLCـ) ةـيـكـلـسـالـلـاـ ةـيـلـحـمـلـاـ ةـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ ةـدـحـوـ يـتـلـاـ ةـمـئـالـمـلـاـ لـيـصـوـتـ مـتـيـ ، مـكـحـتـلـاـ ةـدـحـوـ ةـطـسـاوـبـ عـداـخـمـلـاـ دـحـأـ حـسـمـ وـأـ فـاشـتـكـاـ مـتـيـ اـمـدـنـعـ رـيـدـصـتـ عـمـ رـيـذـحـتـ دـحـاـوـ . SNMPـ ةـدـيـصـمـ تـالـبـقـتـسـمـ عـيـمـجـ ئـلـاـ تـاـمـوـلـعـمـلـاـ هـذـهـ يـلـعـ يـوـتـحـتـ ثـادـحـأـلـاـ نـإـفـ ، عـداـخـمـلـاـ سـفـنـ نـعـ ةـدـدـعـتـمـلـاـ مـكـحـتـلـاـ تـادـحـوـ تـفـشـكـ اـذـاـ هـنـأـ وـهـ SNMPـ رـبـعـ ثـادـحـأـلـاـ دـنـعـ طـقـفـ طـاـبـتـرـالـاـ لـمـعـ مـتـيـ ثـيـحـ NMSـ ةـطـسـاوـبـ اـهـتـيـفـرـ مـتـيـ ةـرـرـكـمـلـاـ PIـ.

## ةـلـيـخـدـلـاـ لـجـسـلـاـ ةـلـهـمـ عـاهـتـنـاـ

ةـيـلـحـمـلـاـ ةـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ رـصـنـعـ تـالـجـسـ ئـلـاـ ةـعـداـخـمـ لـوـصـوـ ةـطـقـنـ ةـفـاضـإـ درـجـمـبـ لـبـقـ نـمـ نـيـوـكـتـلـلـ ةـلـبـاـقـ ةـلـهـمـ دـعـبـ . ةـيـئـرمـ دـوعـتـ اـلـ يـتـحـ كـانـهـ يـقـبـتـ ، (WLCـ) ةـيـكـلـسـالـلـاـ ةـئـفـلـاـ يـفـ قـرـامـ ةـيـحـاـلـصـ تـهـتـنـاـ ، (يـضـاـرـتـفـاـلـكـشـبـ ةـيـنـاثـ 1200ـ) مـدـخـتـسـمـلـاـ

قـيـبـطـتـ مـتـيـ يـتـحـ\_FRIENDLYـ وـ\_CONTAINEDـ لـثـمـ يـرـخـأـلـاـ لـوـدـلـاـ يـفـ دـاغـوـأـلـاـ رـمـتـسـتـ

مەرۆھەظ ۋەداعى ۋەلەح يەھىلۇ بىسانملا فىيەنلىك تىلا.

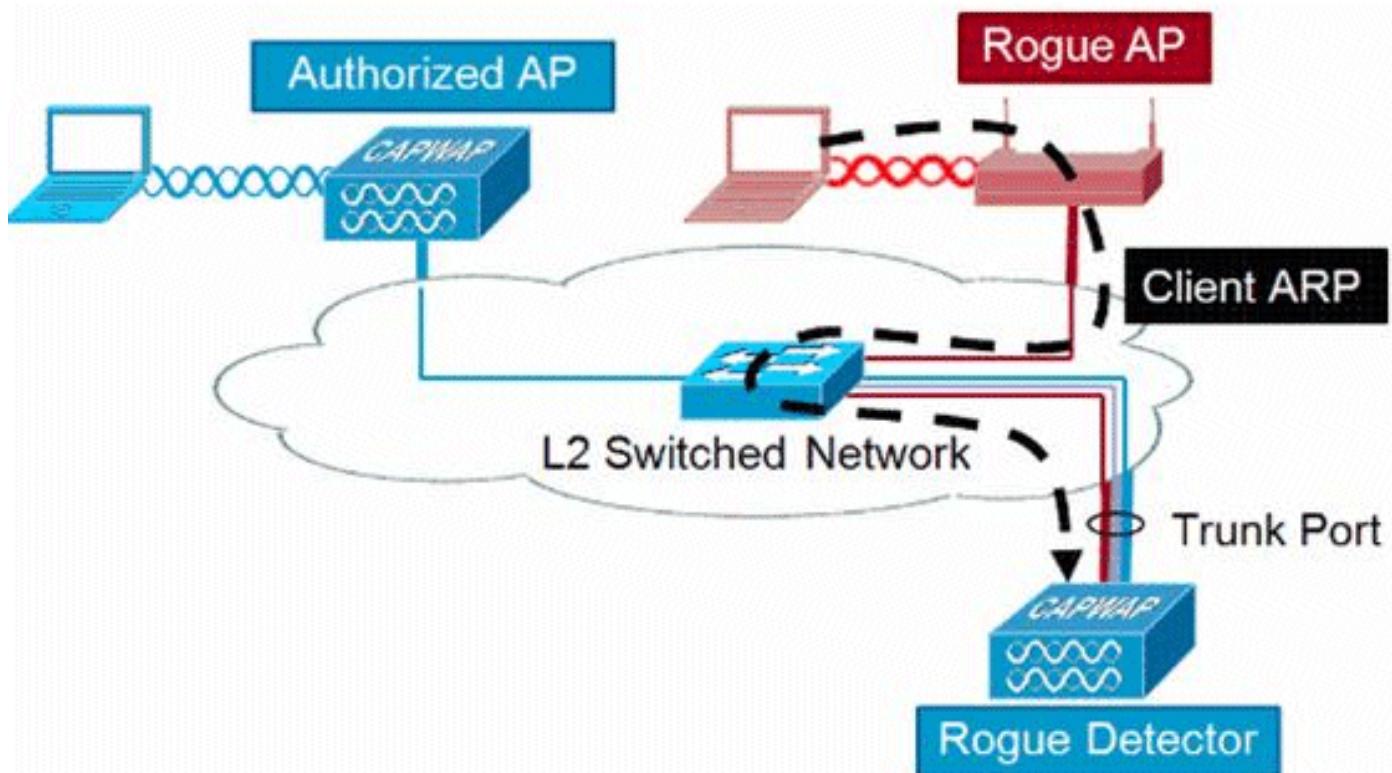
ةمظنألا ربع ريغت يتلارع داخل سلل تانايبلالا ةدعاق مجحل يصقألا دحلا كانه  
مكحتلارع دحول ئيساسألا:

- عداخم لي مع 1500 و ئەلېخد لوصو ئەطقن 600 ئىلا لصى ام ئاوتخاۋاشتىكا - مەئاوتخاۋار قىرام لي مع 32000 و ئەلېخد لوصو ئەطقن 24000 ئىلا لصى ام فاشتىكا
  - 5520
  - 8540

## ع داخمل ا فش اکل لوصول ا ةطقن

عاوهلا ربع اهيلع لوصحلا متي يتلا ئعدا خملاتامولعملاءنراقم (AP) لوص و ئطقن فدهت ئكبشلا نم اهيلع لوصحلا متي يتلا (ARP) نيوانعلاليلحت لوكتورب تامولعمب عامس مت وعداخم ليمع وأ لوص و ئطقن هنأيلع عاوهلا ربع MAC ناوونع عامس مت اذا . ئيكلسلا ئيكلسلا ئكبشلا ئيلع نوكتل اهديدحت متييس عدا خملانإف ، ئيكلسلا ئكبشلا ئيلع اضيأ هي بنتللا ٽروطخ ىوتسم عفر متييس ف ، ئيكلسلا ئكبشلا ئيلع عدا خملادوجوفاشتكا مت اذا ريج عدا خملافشتكمب ئصاخلا لوصولا ئطقن critical\_ئيلار ئعدا خملاتامولعملاءنراقم (NAT) مدخلتسyi زاهج فلخ نيعدا خملاءالاعمال ئيلع فرع تللا يف ٽهجان

اما ،ةقداصملا لاكشأ نم لكش ةعدا خملال وص ول ا ةطقنل نوك ي امدنع بولسألا اذه مدخلتسى نكمي ال ،ةعدا خمل (AP) لوص و ةطقن ىلع ةقداصم جذونم نويوكت مت ي امدنع WEP و A WPA . تاناي ب و ةقداصملا بولسأ فرعت ال اهنأ نارتقالا Lightweight عض ول ا يف لوص ول ا ةطقنل ةعدا خمل (AP) لوص ول ا ةطقن ىلع اهن يوكت مت يتلا دامت غالا.



1

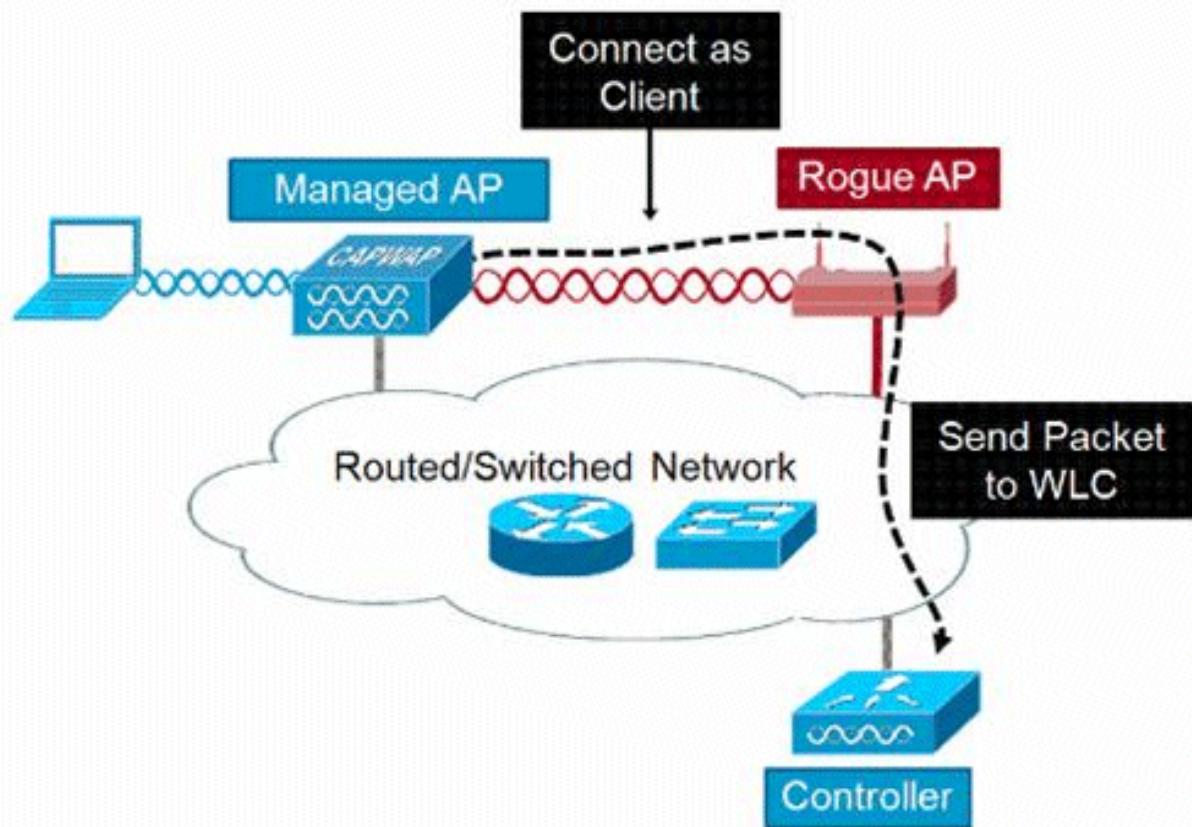
ةع داخم فشك ۋەچەجاك طقىف 1 ۋەچوملا نم لوصولى طاقۇن نىيوكت نكىمى: ئەظەحالىم.

## ةعسوتل ا ةيلباق تارابتع

مٽ اذا .ع داخم لي مع 500 و ع داخم 500 ى لاصي ام فاشتاكا ٽعد داخملالوصول ا طق نل نكمي  
مت ي هن اف ، ٽعد داخملالا ٽزه جألا نم دي دعلالا ى لع يوتحي لاصتا طخ ى لع ع داخملالا فشكلا زاهج عضو  
لوصولالا طاقن ب ظفتحا ، اذه ثودح عن مل .لكل اشم ثودح يف ببستي امم ، دودحلالا هذه زواجت  
كتكبش يف لوصولالا وا عي زوتلا ٽقبط يف راودلalا فشتكمملل.

RLDP

ةلصتم ةنيداعم ٤ع داخم (AP) لوصو ٤طقن تناك اذا ام ديدحت ىلـ RLDP لوكوتورب فدهي (AP) لوصو ٤طقن برقا يس اسأ لكشب ٤زيملا هذه مدخلتست .ةيكسلـا ئيساسـا ئـينـبلـاب ناونـع عم ٤مزـح لـاسـراـ مـتـيـ ،ـليـمعـكـ لـاصـتـالـاـ دـعـبـ يـكـسـالـ لـيـمعـكـ رـاوـدـلـاـ زـاهـجـلـابـ لـاصـتـالـلـ تـنـاكـ اذاـ اـمـ مـيـيـقـتـلـ (WLC) ئـيـكـسـالـلـاـ ئـيـلـحـمـلـاـ ئـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ ئـدـحـوـبـ صـاخـلـاـ ئـهـجـوـلـاـ ئـكـبـشـلـاـ ئـلـعـ عـداـخـمـلـاـ دـوـجـوـ فـاشـتـكـاـ ئـلـاحـ يـفـ .ةـيـكـسـلـاـ ئـكـبـشـلـابـ ئـلـصـتـمـ لـوـصـوـلـاـ ئـطـقـنـ ىـوـتـسـمـ ىـلـاـ هـذـهـ ٤ـعـداـخـمـلـاـ لـوـصـوـلـاـ ئـطـقـنـلـ هـيـبـنـتـلـاـ ئـرـوـطـخـ ىـوـتـسـمـ عـفـرـ مـتـيـ ،ةـيـكـسـلـاـ رـيـطـخـ.



## انه RLDP ۆي مزراوخ درس متي

1. راش إلأ ٰوق ميٰق مادختس اب ع داخملأا إلأ ٰدحوم لوص و ٰطقن برقاً ٰيلع فرعٰتلا.

تايي عمج ثالث لخدتو، WLAN، ٰكبسيل لي معك فلاخملاب لوصولـا ٰطقـن لـصـتـتـ كلـذـ دـعـبـ. تـقولـا يـهـتـنـيـ نـأـ لـبـقـ.

3. نـاـونـعـ لـانـيـ نـأـ لـمـعـتـسـيـ apـ نـإـفـ،ـ نـاـرـتـقـاـ حـجـنـ اـذـاـ.

4. لـسـرـتـ (WLAN) لـيـمـعـكـ لـمـعـتـ يـتـلـاـ) لـوـصـولـاـ ٰطـقـنـ نـإـفـ،ـ IPـ نـاـونـعـ ىـلـعـ لـوـصـحـلـاـ مـتـ اـذـاـ. مـكـحـتـلـاـ ٰدـحـوـلـاـ IPـ نـاـونـعـ لـكـ ىـلـاـ ٰمـزـحـ.

5. اـذـهـ ىـلـعـ ٰمـالـعـ عـضـوـمـتـيـفـ،ـ لـيـمـعـلـاـ نـمـ RLDPـ مـزـحـ نـمـ ٰدـحـاـوـ ٰمـزـحـ مـكـحـتـلـاـ ٰدـحـوـتـقـلـتـ اـذـاـ. ٰغـلـابـ ٰرـوـطـخـ عـمـ كـالـسـأـلـابـ لـصـتـمـ زـاهـجـكـ عـدـاخـمـلـاـ صـخـشـلـاـ.

---

 ئـيـفـصـتـلـاـ دـعـاـوـقـ دـوـجـوـ ٰلـاحـ يـفـ مـكـحـتـلـاـ ٰدـحـوـ ىـلـاـ ٰلـوـصـولـاـ RLDPـ مـزـحـ ىـلـعـ رـذـعـتـيـ:ـ ٰظـاحـاـلـمـ رـاـوـدـلـاـ زـاهـجـلـاـ اـهـ بـ دـجـوـيـ يـتـلـاـ ٰكـبـشـلـاـوـ ٰمـكـحـتـلـاـ ٰدـحـوـ ٰكـبـشـ نـيـبـ.

---

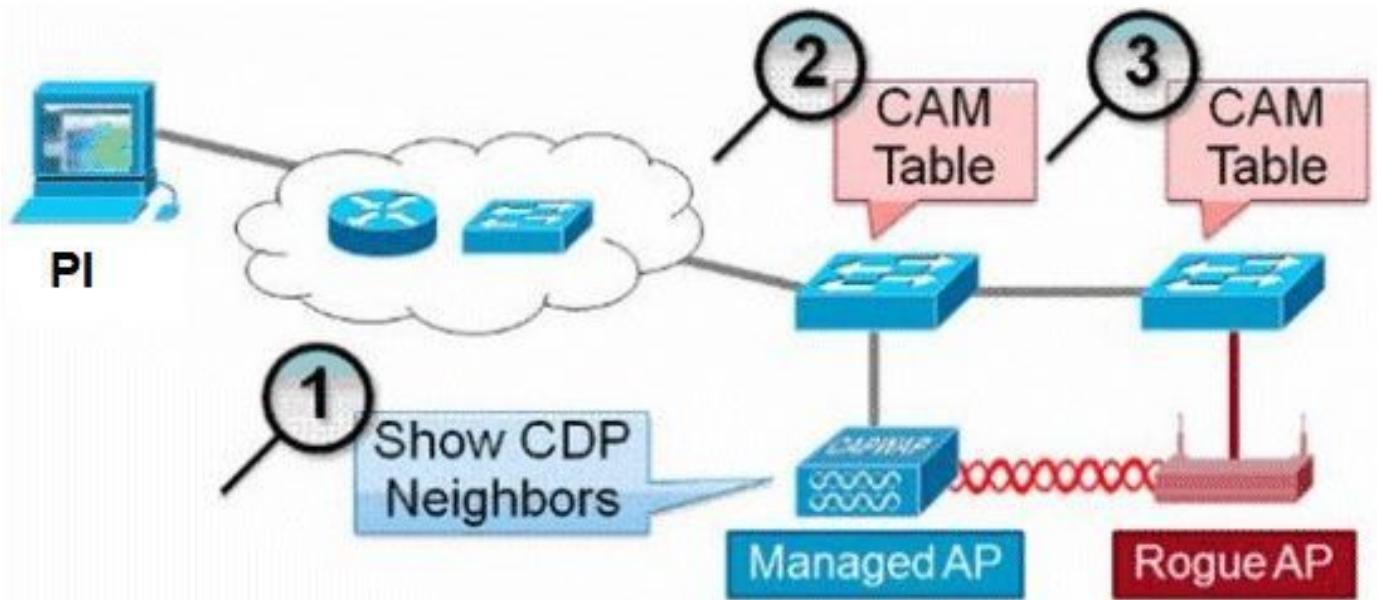
## RLDP تاظفحـتـ

- SSID ثـبـتـ يـتـلـاـ ٰحـوـتـفـمـلـاـ ٰعـدـاخـمـلـاـ لـوـصـولـاـ طـقـفـ RLDPـ لـوـكـوـتـوـرـبـ لـمـعـيـ. رـيـفـشـتـلـاـوـ ٰقـدـاـصـمـلـاـ لـيـطـعـتـ عـمـ اـهـ ٰصـاخـلـاـ.
- لـوـصـحـلـاـ ىـلـعـ ٰرـدـاـقـ لـيـمـعـكـ لـمـعـتـ يـتـلـاـ ٰرـاـدـمـلـاـ لـوـصـولـاـ ٰطـقـنـ نـوـكـتـ نـأـ RLDPـ بـلـطـتـيـ ٰعـدـاخـمـلـاـ ٰكـبـشـلـاـ ىـلـعـ DHCPـ رـبـعـ IPـ نـاـونـعـ ىـلـعـ
- تـارـمـ ٰدـعـ قـرـامـ ىـلـعـ RLDPـ عـبـتـتـ ٰلـوـاحـمـلـ يـوـديـلـاـ RLDPـ مـادـخـتـسـاـ نـكـمـيـ.
- ىـلـعـ اـبـلـسـ اـذـهـ رـثـؤـيـ.ـ عـاـلـمـعـلـاـ ٰمـدـخـ (AP)ـ لـوـصـولـاـ ٰطـقـنـ ىـلـعـ رـذـعـتـيـ،ـ RLDPـ ٰيـلـمـعـ يـفـ يـلـحـمـلـاـ عـضـوـلـاـ يـفـ لـوـصـولـاـ طـقـنـلـ لـاـصـتـاـلـاـوـ ٰعـادـأـلـاـ.
- 5 ٰعـرـسـبـ DFSـ ٰقـاـنـقـ يـفـ لـمـعـتـ ٰعـدـاخـمـ لـوـصـوـنـبـ لـاـصـتـاـلـاـ RLDPـ لـوـكـوـتـوـرـبـ لـوـاحـيـ الـ زـتـرـهـاـجـيـجـ.

## لـوـحـمـلـاـ ذـفـنـمـ تـارـاسـمـ

عـدـبـ مـتـيـ 5ـنـمـ مـغـرـلـاـ ىـلـعـوـ.ـ ٰعـدـاخـمـلـاـ لـوـصـولـاـ ٰطـقـنـ فـيـفـخـتـ ٰيـنـقـتـ وـهـ لـوـحـمـلـاـ ذـفـنـمـ عـبـتـتـ ىـلـعـ SNMPـ لـوـكـوـتـوـرـبـوـ CDPـ دـامـتـعـاـ تـانـاـيـبـ نـأـ نـمـ مـغـرـلـاـ ىـلـعـ.ـ DMTUـاـ TـA~I~B~ مـادـخـتـسـاـبـ ٰعـارـقـلـلـ دـامـتـعـاـ تـانـاـيـبـ نـأـ نـمـ مـغـرـلـاـ ىـلـعـ.ـ SNMPـ دـامـتـعـاـ تـانـاـيـبـ مـادـخـتـسـاـبـ ٰعـارـقـلـلـ دـامـتـعـاـ تـانـاـيـبـ نـأـ نـاـ،ـ ٰقـرـامـلـاـ ٰشـاشـلـاـ يـفـ ٰلـيـغـشـتـ مـتـيـ يـذـلـاـ ذـفـنـمـلـاـ فـيـرـعـتـلـ ىـلـعـ يـوـتـحـتـ يـهـفـ يـلـاـتـلـابـوـ،ـ اـضـيـأـ ذـفـنـمـلـاـ لـيـغـشـتـ فـاقـيـإـابـ PIـ ٰكـرـشـلـ حـمـسـتـ ٰبـاتـكـلـاـوـ دـيـدـهـتـلـاـ.

عـمـ Cisco IOS® جـمـانـرـبـ لـغـشـتـ يـتـلـاـ Ciscoـ تـالـوـحـمـ عـمـ طـقـفـ ٰزـيـمـلـاـ هـذـهـ لـمـعـتـ،ـ تـقـوـلـاـ اـذـهـ يـفـ ٰرـاـدـمـلـاـ لـوـصـولـاـ طـقـنـ ىـلـعـ (APs)ـ CDPـ نـيـكـمـتـ بـجـيـ اـمـكـ.



انه لوحملاء ذفنم عبنت ئيمزراوخ درس متى:

لوصولا ئطقن فشتكت يتل او، لوصو ئطقن برقاً (PI) تىرنىلا لوكوتورب دجي و. 1. لوكوتورب يف اهتاراج عجرتسى تو، ئاوهلا ربعة داخملاء CDP.

ثحبىف، رواجملا لوحملاء لخاد CAM لوكوتورب PI مدخلتسى كلذ دعبو. 2. داخملاء عقوم ديدحتلى يباجيما قباتات نع.

يأ، داخملاء MAC ناونع +1/1، امامت داخملاء MAC ناونع ىلعي باجيما قباتات دمتعت - . 3. ئلصأتىملا دروملا تامولعم ىلا ادانتسا WI قباتات وأ، نىع داخملاء ئالىمعلل MAC ناونع يف MAC.

حاتفم رواجم يف ثحبلا لصاوى PI لا، حاتفم برقا ىلعي باجيما قباتات ىلعي مل نا. 4. (ايضارتغا) ادىع ب ئكىن ئانثا ىلا.

# Wired-Side Tracing Techniques

## Comparison

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

## نیقرامل افینصت

Cisco UWN طس اوپ اهن ع فشكلا مث يتلا عاطخألا عي مج رابتغا متي، يضارتفا لکش ب نم ددع ىلع ءانب عاطخألا فینصت نكمي، مسرلا اذه يف حضوم وہ امك. فنصم ریع: عالملان ددعو ةكبشلا فاقیا/لیغشتونامألا عونو RSSI و SSID نمضتت يتلا ریياعملان

Lower Severity

Higher Severity

Off-Network  
Secured  
Foreign SSID  
Weak RSSI  
No clients

On-Network  
Open  
Our SSID  
Strong RSSI  
Attracts clients

## نېقراډلا فېنڅت دع اووق

ىلע عداخملा زیمېت پېتلما طورشلا نم ټعومجډ فېرعتب کل حمسټ، ټعداخملاء فېنڅتلا دع اووق ڈھو ىلع اړئاد اه ڏيغې فنت متي اهنکلو، WLC وا PI یف دع اووقلا هذه نېوکت متي. ېدو وأ راض هنأ ډي ډي ټعداخملاء فاشتکا دنډ مکحتلا.

**ټکبېشلا یف مکحتلا تادحو یف تادنټس ملأا ټدعاق ىلإ دنټس ملأا ټغوارملاء فېنڅت أرقا** نم دېزم ىلع لوصحلل (PI) ټيساسألا ټينبل او (WLC) ټيکلساللا ټيلحملاء (WLC).

## HA ټئاچ

هذه نېزخت متي، ټلهس ټلاح وا (ټئف يأ) ټاوتحم ټلاح ىلإ ايودي ټعداخملاء زاهج يأ لقنب تممق اذا تانايبلاء ټدعاق ٿي ڏوخت متي ال، کلذ عموم، ټي طايتحالا Cisco WLC flash ټركاڙ یف تامولعملاء لوحملاب ټصالخلا Flash ټركاڙ نم ټعداخملاء ټمئاقلاء ليمحت متي، HA ليدبت ٿدھي امدنع (WLC) قباسلا ټي طايتحالا Cisco WLC.

وا "يلاع" ىلإ "عداخملاء نع فشكلا" ناما ټوتس نېييعت متي اذا، "يلاعلا رفوتلاء" وي رانيس یف تېبېثت تقو ډعب طقف ټي طايتحالا مکحتلا ڈھو ىلع دوچو ټڪنلوجۍ دادع أدبي، "ماه" سکعنېت ال، ټيلاتلابو. ټيناث 300 غلبې یذلابو، ټعداخملاء نع فشكلا تالوحملاب ټي بېثت ټيناث 300 ډعب ال ټي طايتحالا مکحتلا ڈھو ىلع ټطشنللا تانېوکتلا.

## نرملا لاصتا ټئاچ

ټمئاچ لصتملا عضولا یف (عداخملاء فشكلا نېيکمت عم) FlexConnect لوصولا ټطقن ڏخأت ىلع ايئا ټڪنلوجۍ ټي وتحت یتلا SSID نم لک نېييعت ټلاح يف. مکحتلا ڈھونم ټاوتحم عيمج ىلع تانېوکتلا هذه نېييعت متي ذئدنعف، مکحتلا ڈھو یف "يئا ټڪنلوجۍ ټاوتحا" ټزيم و هذه نېزختب لوصولا ټطقن موقتو لصتملا عضولا یف FlexConnect لوصولا طاقن اه ټركاڙ یف تانېوکتلا.

ذېفنېت متي، لقتسملا عضولا ىلإ FlexConnect نم (AP) لوصولا ټطقن لقتښت امدنع: ټيلاتلما ماهملاء:

- ټرمتس م بقارملاء اه عضو یتلا ټاوتحالا ټيلمع لازت الو.

- سفن ىلع ټي وتحت ټعداخملاء لوصولا ټطقن تفشتكا اذا لېصوت متي یتلا مکحتلا ڈھو یف SSID نېوکت متي SSID نم ض دوچو ټڪنلوجۍ فرع SSID ټاوتحالا نېيکمت متي اذا ټاوتحالا عدب متي سف، اهاب FlexConnect لوصولا ټطقن لقتسملا عضولا ىلإ اه کيرحت لباق مکحتلا ڈھونم ټئا ټڪنلوجۍ.

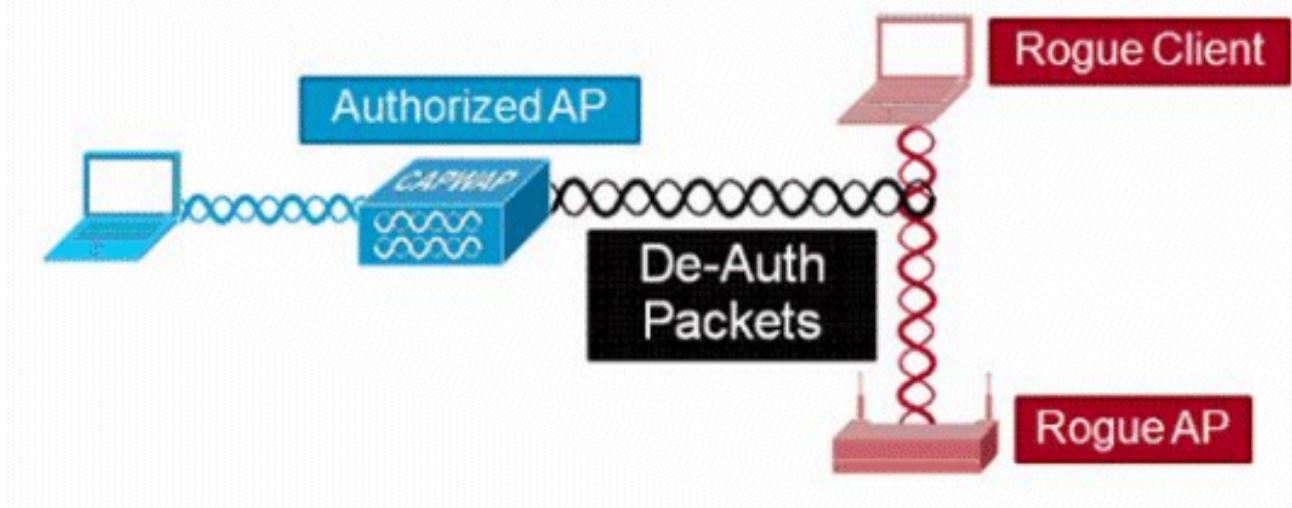
- ټزيم نېيکمت متي اذا ټاوتحالا أدبي، نارقاً راود يأ FlexConnect لوصولا ټطقن تفشتكا اذا لصتملا عضولا یف تناناک امدنع مکحتلا ڈھونم "يئا ټڪنلوجۍ ټاوتحالا".

متي، لصتملا عضولا ىلإ ټرم FlexConnect AP ټلقتسملا لوصولا ټطقن لقتښت امدنع ماهملاء هذه ذېفنېت:

- ټاوتحالا عيمج حسم متي.

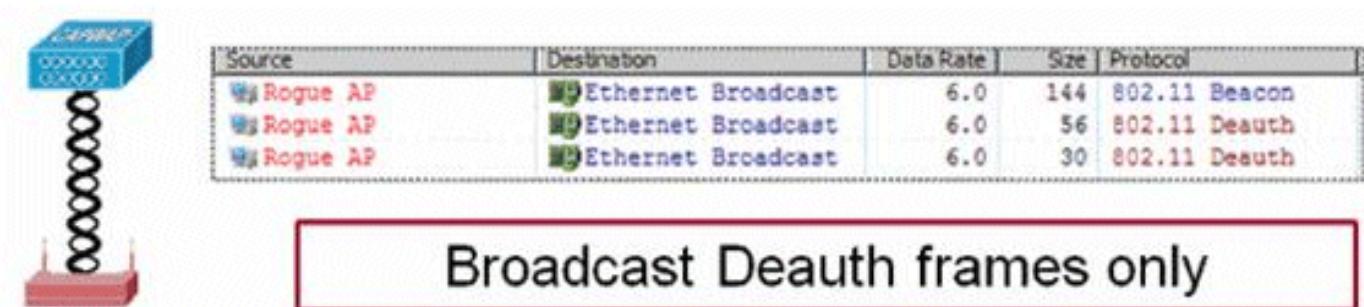
## ةع داخمل ا رطاخمل ا في فخت

نیع داخمل ا عاوتحا

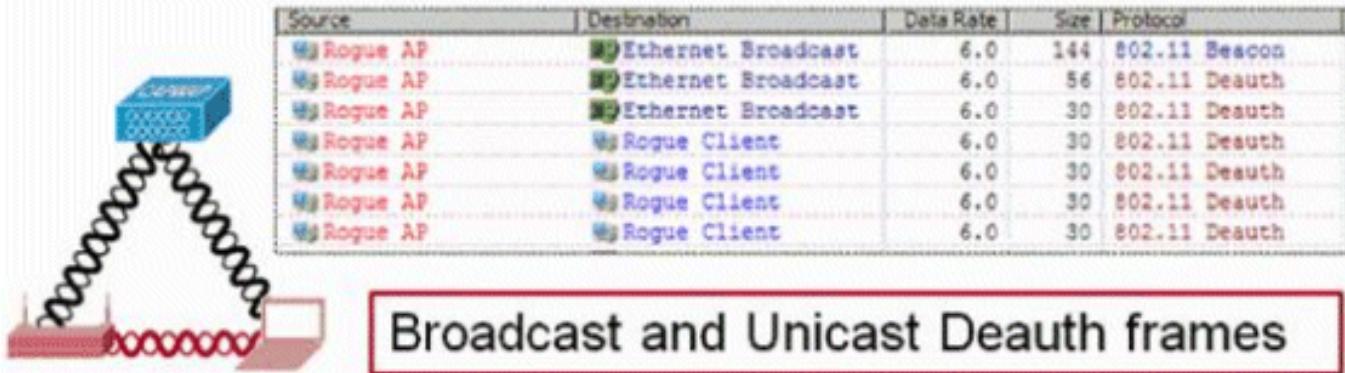


## ڦع داخملاء او تحالا لي صافت

نودب ۃع داخم (AP) لوص و ۃطقن یل ع اهل یغشت عدب متي یتل اعاوتح الۃ یيل مع مدخلت سرت ال  
ثبلأا ناونع یل اهل اسرا متي یتل اوق داصمل ااغل تاراطا الی عالم



وقاصملاءاغلitarاطامادختساعمدعداخم(طاقدن)لوصوطةقندلعاوتحالاعدبمتيليمعلانويوانعيلاوتبلاناونعنيلةلسرملا:



نكمم لدعم لقأو ةرادملأا لوصولـا ئطقـن ئقاطـى وتسـمـى لـعـاـوتـحـاـلـاـ مـزـحـ لـاسـرـاـ مـتـيـ تـانـايـبـلـلـ

ةـينـاثـ يـلـلـمـ 100ـ لـكـ لـقـأـلـاـ لـعـاـوتـحـوـ ئـيـتـدـحـوـ ئـاـوتـحـاـلـاـ لـسـرـتـ

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

~100ms

بـقـارـمـلـاـ رـيـغـ عـضـوـلـاـ يـفـ لـوـصـوـلـاـ طـاقـنـ لـبـقـ نـمـ ھـوـارـجـاـ مـتـيـ ئـاـوتـحـاـلـاـ مـتـيـ ئـظـحـاـلـمـ يـلـلـمـ 100ـ غـلـبـيـ يـذـلـاـ يـنـمـزـلـاـ لـصـافـلـاـ نـمـ الـدـ ھـيـنـاـثـ يـلـلـمـ 500ـ اـهـرـدـقـ ھـيـنـمـزـ ھـرـتـفـ يـفـ بـقـارـمـلـاـ عـضـوـلـاـ عـضـوـيـفـ لـوـصـوـلـاـ طـاقـنـ لـبـقـ نـمـ مـدـخـتـسـمـلـاـ ھـيـنـاـثـ

- لمـعـتـ ةـرـادـمـ لـوـصـوـ طـاقـنـ 4ـ ىـلـاـ 1ـ نـيـبـ اـمـ لـالـخـ نـمـ يـدـرـفـ عـدـاخـمـ زـاهـجـ يـأـ ئـاـوتـحـاـلـاـ نـكـمـيـ
- تـقـؤـمـ لـكـشـبـ دـيـدـهـتـلـاـ فـيـفـخـتـلـ نـارـتـقـإـلـابـ

- ةـبـقـارـمـلـاـ عـضـوـوـيـلـحـمـلـاـ عـضـوـلـاـ يـفـ لـوـصـوـلـاـ طـاقـنـ مـادـخـتـسـابـ ئـاـوتـحـاـلـاـ ذـيـفـنـتـ نـكـمـيـ
- تـاذـ لـوـصـوـلـاـ طـاقـنـلـ يـلـحـمـلـاـ عـضـوـلـلـ ھـبـسـنـلـابـ .(لـصـتـمـلـاـ)ـ نـرـمـلـاـ لـاـصـتـالـاـ عـضـوـوـ
- يـكـلـسـالـ زـاهـجـ لـكـلـ ھـيـصـقـأـ دـحـكـ ھـعـدـاخـمـ ھـزـھـجـأـ ھـثـالـثـ ئـاـوتـحـاـلـاـ نـكـمـيـ ،نـرـمـلـاـ لـاـصـتـالـاـ
- دـحـكـ ھـعـدـاخـمـ ھـزـھـجـأـ ھـتـسـ ئـاـوتـحـاـلـاـ نـكـمـيـ ،ةـشـاشـلـاـ عـضـوـيـفـ لـوـصـوـلـاـ طـاقـنـلـ ھـبـسـنـلـابـ
- يـكـلـسـالـ زـاهـجـ لـكـلـ ھـيـصـقـأـ

## يـئـاـقـلـتـ ئـاـوتـحـاـ

ةـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ ھـجـاـوـ وـأـ PـIـ رـبـعـ عـدـاخـمـ زـاهـجـ ىـلـعـ اـيـوـدـيـ ئـاـوتـحـاـلـاـ عـدـبـ ىـلـاـ ھـفـاضـإـلـابـ عـدـبـ ىـلـعـ ھـرـدـقـلـاـ اـضـيـأـ كـانـھـ ،WLCـ )ـ ئـيـكـلـسـالـلـاـ ھـيـلـحـمـلـاـ ھـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ ھـدـحـوـبـ ھـصـاـخـلـاـ مـسـقـ نـمـضـ نـيـوـكـتـلـاـ اـذـهـ ىـلـعـ رـوـثـعـلـاـ مـتـ .ةـنـيـعـمـ تـاـهـوـيـرـانـيـسـ لـظـ يـفـ اـيـئـاـقـلـتـ ئـاـوتـحـاـلـاـ لـكـشـبـ تـازـيـمـلـاـ ھـذـھـ نـمـ لـكـ لـيـطـعـتـ مـتـيـ .مـكـحـتـلـاـ ھـدـحـوـ ھـھـجـاـوـ وـأـ PـIـ ھـجـاـوـلـ ھـعـدـاخـمـلـاـ تـاـسـاـيـسـلـاـ رـرـضـ رـبـكـأـ بـبـسـتـ يـتـلـاـ تـاـدـيـدـهـتـلـاـ لـاـطـبـإـلـ طـقـفـ اـهـنـيـكـمـتـ بـجـيـوـيـضـاـرـتـفـاـ

- ةـكـبـشـلـابـ لـصـتـمـ ھـنـأـبـ عـدـاخـمـ زـاهـجـ ىـلـعـ فـرـعـتـلـاـ ھـلـاحـ يـفـ - كـلـسـلـاـ رـبـعـ ھـعـدـاخـمـلـاـ ئـاـوتـحـاـلـاـ تـحـتـ اـيـئـاـقـلـتـ ھـعـضـوـيـ مـتـيـ ،ئـيـكـلـسـلـاـ

- نوكمل ا فرع ملل لثامم SSID مدخلتسي راودلا زاهجلاناك اذا - انب صالحا SSID مدخلتسي موجه ةجلاع مىلا ةزيمل ا هذه فدهتو . ايئاقت هئاوتحا متى هناف ، مكحتلا ةدحوىل عرضلا ثودح يف ببسنت نأ لباق لسعلا تيزب.
- RADIUS/AAA مداخ يف جردم ليمع نأ جو اذا - ةليخدلا لوصولا ةطقن ئل ع حلاص ليمع نارتقا نم هعنمي و ، طقف ليمعلا كلذ دض ءاوتحالا ليغشت متى ، عداخم زاهجب طبترم ةرادم ريغ (AP) لوصو ةطقن يأ مىلا
- اهءاوتحا متى ، نارقأ ةكبش فاشتكا ةلاح يف - ةصصخمل ا ةعداخمل ا لوصولا ةطقن ايئاقت

## قراهم ءاوتحا

- ءاغلإ تاراطإ لاسرايل ةرادمل ا لوصولا ةطقن ويدار تقو نم اعزج مدخلتسي ءاوتحالا نألو ةبسنب يبلس لكشب رثأتى توصل او تانايبل ا ءالمع نم لك كل ءادالا نإف ، ةقداصمل ا ةبسنلاب جرخلا يف لقا ريثأتلا نوكى ، تانايبل ا ءالمع ةبسنلاب 20٪ ئل ا لصت ةدوغ ليلىقت و تاثداحمل ا يف تاعطاوم ثودح يف ءاوتحالا ببستي دق ، توصل ا ءالمع توصللا
- نم دكأت . ةرواجمل ا تاكبشلا دض هقالطإ متى امدنع ةينوناق تايعادت ءاوتحا ل نوكى دق . ءاوتحالا ةيلمع عدب لباق ةينمأ رطاخم لكشىو كتكبش لخاد دوچوم عداخمل ا زاهجلانأ

## لوجهلا ذفنم ليغشت فاقيا

ىل ع بجي . PI يف ءانيم نأ زجعي نأ رايح كانه SPT ، نملامعتسىالا ب ءانيم حاتفم عبtti نا ام ةلما زتمت اذا PI لالخ نم لوجهلا ذفنم نيكمتل رايح رفوتى . ايودي بيمرتللا اذه عارج ا لوفسملا ةكبشلا نم ايلعف ييقاولما

## نيوكتل

### عاطخألا نع فشكلا نيوك

يضارتفا لكشب مكحتلا ةدحو يف عداخمل ا فشكلا نيكمت متى .

> ةيكلساللا ةيامحلا تاسايس < نيمأتلا ئل ا لقتنا ، ةفلتخم تاريح نيوكت لجأ نم لاثمل ا ليبس ئل ع . ةمامع > ةعداخمل ا تاسايسلا :

ةعداخمل ا لوصولا طاقنل ئلهمل ا ربيغت . 1. ةوطخل

ةتقؤمل ا ةعداخمل ا تاكبش فاشتكا نيكمت . 2. ةوطخل

**CISCO**

Sys Configuration | Ping | Logout | Refresh

**MONITOR** **WLANS** **CONTROLLER** **WIRELESS** **SECURITY** **MANAGEMENT** **COMMANDS** **HELP** **FEEDBACK** **Home**

## Security

### Rogue Policies

**Rogue Detection Security Level**

<input type="radio"/> Low	<input type="radio"/> High	<input type="radio"/> Critical	<input checked="" type="radio"/> Custom
Rogue Location Discovery Protocol	AllAps		
Expiration Timeout for Rogue AP and Rogue Client entries	3600 Seconds		
Validate rogue clients against AAA	<input type="checkbox"/> Enabled		
Validate rogue AP against AAA	<input type="checkbox"/> Enabled		
Polling Interval	0 Seconds		
Validate rogue clients against MSE	<input type="checkbox"/> Enabled		
Detect and report Ad-Hoc Networks	<input checked="" type="checkbox"/> Enabled		
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	<input type="checkbox"/> Enabled		

---

### Auto Contain

Auto Containment Level	Auto
Auto Containment only for Monitor mode APs	<input type="checkbox"/> Enabled
Auto Containment on FlexConnect Standalone	<input type="checkbox"/> Enabled
Rogue on Wire	<input type="checkbox"/> Enabled
Using our SSID	<input type="checkbox"/> Enabled
Valid client on Rogue AP	<input type="checkbox"/> Enabled
Advises Rogue AP	<input type="checkbox"/> Enabled

رماؤلا رطس ٥٥ جاونم

<#root>

(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
```

ع دا خ م ل ا ن ع ف ش ك ل ل ة ان ق ل ا ص ح ف ن ي و ك ت

نیوکت نموض رایخ کانه Flex-Connect/Monitor، یل حمل اعضولا نم لوصل ۃطقنل ۃبسنلاب یل ع دمتعی لال ظلل اییوض احسم متی یتل اتاونقل رایتخاب مدختسملل حمسی RRM نیع داخملانع اثحب DCA ۃانق/دلبل/ۃانقل لک لوصل ۃطقن حسمت و، نیوکتل

یف حضوم وه امک، ماع>802.11a/802.11b>RRM in order to تلکش يكلاس اال، gui، لـا نم اذه تلکش روصلا.

Wireless

802.11a > RRM > General

**Profile Threshold For Traps**

- Interference (0 to 100%)
- Clients (1 to 200)
- Noise (-127 to 0 dBm)
- Utilization (0 to 100%)

**Noise/Interference/Rogue/CleanAir Monitoring Channels**

Channel List	Country Channels ▾
Monitor Intervals (60 to 3600 secs)	All Channels
	Country Channels (selected)
	DCA Channels

- Channel Scan Interval: 180
- Neighbor Packet Frequency: 180
- Neighbor Timeout Factor (5 to 60): 20

**Factory Default**

Set all Auto RF 802.11a parameters to Factory Default.

**Foot Notes**

رم أول رطس ٰج او نم:

<#root>

(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

ع داخمل ا فينصت نيوكت

ا يودي ٰع داخلم لوصو طقون فينصت

ع داخلم > Monitor ىلإ لقتنا ، فنصم ريج وأ ظارض وأ ظارض (AP) لوصو طقون فينصت لجأ نم رتخا . نيعمل ا ٰع داخمل ا لوصول ا ظقون مسا قوف رقناو ، فنصم ريج (AP) لوصو طاقن > ظوصل ا يف حضوم وه امك ، ظل دسنملا ظمه اقل ا نم رايخل ا.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK < Back Apply Home

**Rogue AP Detail**

Summary	MAC Address	00:06:91:43:6d:e2					
Access Points	Type	AP					
Cisco CleanAir	Is Rogue On Wired Network?	No					
Statistics	First Time Reported On	Thu May 30 16:21:30 2019					
CDP	Last Time Reported On	Fri May 31 13:07:11 2019					
Rogues	Class Type	Unclassified ▾					
Friendly APs		Friendly					
Malicious APs		Malicious					
Custom APs		Unclassified					
Unclassified APs		Custom					
Rogue Clients	State						
Adhoc Rogues	Manually Contained	No					
Friendly Adhoc	Update Status	-- Choose New Status -- ▾					
Malicious Adhoc							
Custom Adhoc							
Unclassified Adhoc							
Rogue AP ignore-list							
Clients							
Sleeping Clients							
Multicast							
Applications							
Lync							
Local Profiling							
<b>APs that detected this Rogue</b>							
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
<a href="#">Clients associated to this Rogue AP</a>							

رم أولاً رطس ٥٥ جاونم:

<#root>

(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 advertising our SSID.
timeout	Configures the expiration time for rogue entries, in seconds.
valid-client	Configures policy for valid clients which use rogue APs.

لوصو طاقن > عداحم > Monitor لى لقتنا ، عداحم ال ظمى اقلا نم ايودي عداحم لاخدا ةلازال .ةروصلان يف حضوم وه امك ، ةلازا قوف رقنا او ، فنصم رينغ

وھفصىلا > عداھملأا نم ۋەھىچىملا ۋەھىچىلەملا ۋەھىچىلەملا تالاخدا نم قىقحتىلا نكىمىي  
ۋەھىچىلەملا يېھىزىملا ۋەھىچىلەملا ۋەھىچىلەملا.

The screenshot shows the Cisco Wireless Controller (WLC) configuration interface under the 'SECURITY' tab. On the left, a navigation tree includes 'AAA', 'Local EAP', 'Advanced EAP', 'Priority Order', 'Certificate', 'Access Control Lists', 'Wireless Protection Policies', 'Rogue Policies', and 'Friendly Rogue'. The 'Friendly Rogue' item is highlighted with a red box. The main panel displays a 'Create' form for a 'Friendly Rogue' entry. It has two fields: 'MAC Address' containing '11:22:33:44:55:66' and 'Type' set to 'Friendly'. Both of these fields are also highlighted with a red box. In the top right corner, there is an 'Apply' button.

## عِدَّاْخُمْلَا فِشْتَكْمَلْ لِوْصَ وَ طَقْنَ نِيْوَكْ

لقتنا ،ةيموسرلا مدخلتسملاءهجاو لالخ نم عدالم فشتكمك لوصولا ةطقن نيوكت لجأ نم ةطقن عضوريغتب مقولوصولا ةطقن مسا رتخا .لوصولا طاقن عي مج > يكلسالىلا .ةروصلالا يف حضوم وه امك لوصولا

The screenshot shows the Cisco Wireless Controller (WLC) interface. In the top navigation bar, the 'WIRELESS' tab is selected. On the left, the 'Access Points' section is expanded, showing 'All APs' selected. The main content area displays the 'General' tab of an AP configuration page. A red box highlights the 'AP Mode' dropdown menu, which lists 'local', 'FlexConnect', 'monitor', and 'Rogue Detector'. The 'Rogue Detector' option is currently selected.

رم أولاً رطس ٥٥ جاو نم:

<#root>

(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

ع داخمل ا فشتكمب ٤صالا لوصول ا ٤طقنل نيوكت SwitchPort

```
interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk native vlan 100
switchport mode trunk
```

---

لـ IP لاصتا ىقلتني نـ ليكشت اـ ذه يـ عـ يـ بـ طـ يـ لـ هـ VLAN لـ اـ ظـ اـ لـ مـ WLC.

---

نيوكت RLDP

لـ قـ تـ نـ اـ ، مـ كـ حـ تـ لـ اـ ٤ـ دـ حـ وـ بـ ٤ـ صـ اـ خـ لـ اـ (GUI) ٤ـ يـ مـ وـ سـ رـ لـ اـ مـ دـ خـ تـ سـ مـ لـ اـ ٤ـ جـ اوـ يـ فـ RLDP نـ يـ وـ كـ تـ لـ جـ اـ نـ مـ لـ قـ مـ اـ عـ > ٤ـ عـ دـ اـ خـ مـ لـ اـ تـ اـ سـ اـ يـ سـ لـ اـ > ٤ـ يـ كـ لـ سـ اـ لـ لـ اـ ٤ـ يـ اـ مـ حـ لـ اـ تـ اـ سـ اـ يـ سـ > نـ اـ مـ اـ لـ اـ لـ اـ .

ةبقارملأا عضويف لوصولـا طاقـنـلـ طـقـفـ حـمـسـيـ -ةـبـقـارـمـلـاـ عـضـوـىـلـاـ لـوـصـولـاـ طـاقـنـلـ يـفـ ةـكـراـشـمـلـابـ RLDP.

-نـرـمـ/ـيـلـحـمـ" عـضـوـىـلـاـ طـاقـنـلـ عـيـمـجـ connect/monitor" يـفـ RLDP.

ايـودـيـ RLDPـ لـيـغـشـتـ مـدـخـتـسـمـلـلـ نـكـمـيـ ،ـكـلـذـعـمـوـ .ـايـئـاـقـلـتـ RLDPـ لـيـغـشـتـ مـتـيـ الـلـطـعـمـ (ـرـمـاـوـأـلـاـ رـطـسـ ـهـجـاـوـ)ـ CLIـ لـالـخـ نـمـ نـيـعـمـ MACـ نـاـونـعـلـ.

لـوـصـولـاـ طـقـنـلـ ءـيـلـصـفـأـلـاـ ئـلـعـ ءـبـقـارـمـلـاـ عـضـوـىـفـ لـوـصـولـاـ طـقـنـلـ لـصـحـتـ ظـاحـاـلـ زـواـجـتـ ةـنـيـعـمـ رـوـمـ ةـلـاحـ اـمـهـنـمـ لـكـ فـشـتـكـاـ اـذـاـ RLDPـ ذـيـفـنـتـلـ اـذـاـ Flex-Connect APـ ةـيـلـحـمـلـاـ -85ـ لـبـيـسـيـدـ RSSIـ.

رمـاـوـأـلـاـ رـطـسـ ـهـجـاـوـ نـمـ:

```
<#root>
(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
```

ايودي RLDP عدل .رم أولا هجوم لالخ نم الا يوديل لغش مل او RLDP لودج نيوكت نكمي ال:

```
<#root>
(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).
```

لودج ةبسنلاب RLDP:

```
<#root>
(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.
```

:رم أولا مادختساب RLDP ۋاحم ئداعى تايىلمۇن نيوكت نكمىي

```
<#root>
(Cisco Controller) >
config rogue ap rldp retries ?
<count>      Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

# عاطخألا فيفخت نيوكت

## يوديلا ءاوتحالا نيوكت

وه امك ،ةفنصم ريق > عداصم > Monitor > لقتنا ،ايودي ظعداضم لوصو ظطقن ءاوتحا لجأ نم روصللا يف حضوم.

The screenshot shows the Cisco Controller's Monitor interface. On the left, a sidebar lists various monitoring categories like Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients, Applications, Lync, Local Profiling, and Cloud Services. Under the 'Rogues' category, 'Unclassified APs' is highlighted with a red box. In the main pane, the title is 'Rogue AP Detail'. It displays details for a rogue client: MAC Address (00:06:91:53:38:20), Type (AP), Is Rogue On Wired Network? (No), First Time Reported On (Tue Jun 4 13:03:55 2019), Last Time Reported On (Tue Jun 4 13:03:55 2019), Class Type (Unclassified), State (Alert), and Manually Contained (No). Below these, there's a 'Update Status' dropdown set to 'Contain' with a red box around it. A red box also highlights the dropdown menu for 'Maximum number of APs to contain the rogue', which includes options like 'Choose Number of APs', 'Auto', and numbers 1, 2, 3, and 4. The number '3' is currently selected. At the bottom, it shows 'APs that detected this Rogue' with a table:

Base Radio MAC	AP Name	SSID	el (MHz)	Radio Type	Security Policy	Pre-Aamble	RSSI
00:27:e3:36:4d:a0	tiagoApCb.98E1.3DEC		1 20	802.11g	Encrypted	Long	-128

رمأولا رطس ٥٥جاونم:

<#root>

(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].



ةدحوم دختسٌت، يضارٌت فا لكشبو. لوصو طاقن 1-4 ب نييعم قرام ءاوتحا نكمي: ةظحالم فاشتكا نم لوصولـا طاقن نم نانثـا نكمـت اذـا. ليـمع ءاوتحـال ةـدحاـلـوـلـوـصـوـةـطـقـنـمـكـحـتـلـاـ لـيـمعـلـاـىـلـعـRـSـIـىـلـعـأـىـلـعـيـوتـحـتـيـتـلـاـ(AP)ـلـوـصـولـاـةـطـقـنـيـوتـحـتـ،ـنـيـعـمـلـيـخـدـ عـضـوـنـعـرـطـنـلـاـضـغـبـ APـ.

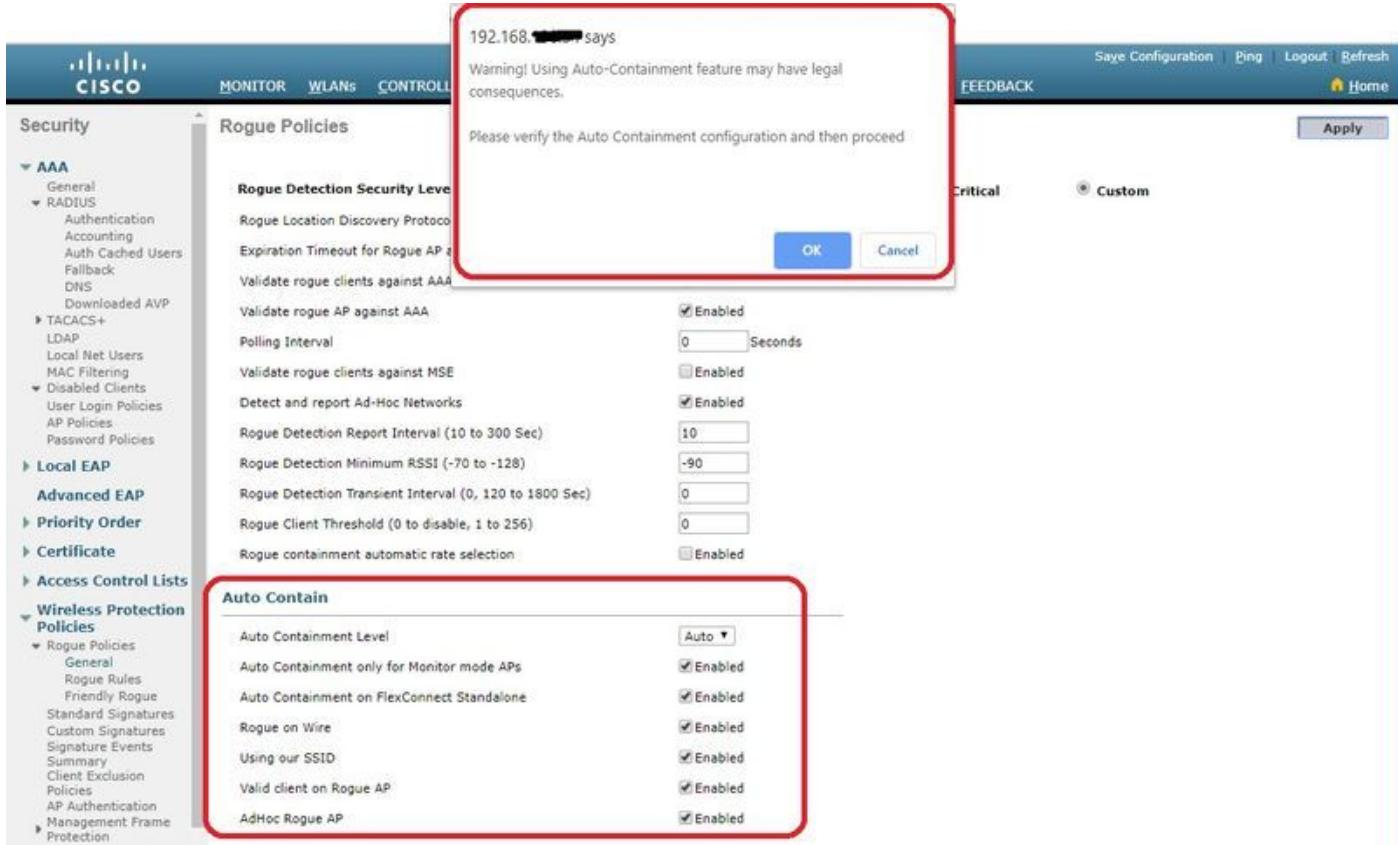
يەقلە ئاوتە

تاس اي سلا> ئي كلس الـ Security ئيلـ اس اي سـ لـ اـ مـ حـ لـ اـ تـ اـ سـ ئـ اـ يـ ئـ اـ قـ لـ تـ لـ اـ عـ اـ وـ تـ حـ اـ لـ اـ نـ يـ وـ كـ تـ لـ كـ تـ كـ بـ شـ ئـ لـ عـ قـ يـ بـ طـ تـ لـ لـ ئـ لـ بـ اـ قـ لـ لـ اـ تـ اـ رـ اـ يـ خـ لـ اـ عـ يـ مـ جـ نـ يـ كـ مـ تـ بـ مـ قـ وـ > ئـ دـ اـ خـ مـ لـ

Cisco نم (WLC) ئىكلساللا ئىلەملا ئەكپشللا يف مەكتەل رەصنۇع يوتحىي نأ دىرت تىنك اذى، ئەدەم رېغ رايىت خالا تاناخ كىرتا، ئالا و. تاعبەرمەلا ھەذە دەحەف، ئەنىيەم ئەلىخ دەزەج أىلۇع اىيەقلىت ئەضارتەفالا ئەمىقلىا يە ئىتلەو.

لعل اي اقلت يوتحت يتلا تاملعمل اي هذه

رتماراب	فصوصوا
عضويف لوصوصوا ضرعلا زاحج	
يئاقلت ئاتخالا FlexConnect ةلقتسملا	ىلع يئاقلتلا ئاتخالا نيكمتل اهديدحت كنكمي يتلا رايتحالا ئناخ ةلود ريققتلا .لقتسملا عضويف FlexConnect نم لوصوصوا طاقن ،لقتسملا عضويف FlexConnect لوصوصوا طاقن نوكت امدنع .قأعم لوصوصوا طاقنل يئاقلتلا ئاتخالا ئادختسا ايـس مـادختـسا نـيكـمـتـ كـنكـمـيـ لـوصـوصـواـ طـاقـنـ ئـطـقـنـ لـاصـتـاـ دـعـبـ ئـاتـخـالـاـ فـقـوـتـيـ .SSIDـ وـأـ ئـعـداـخـمـلـاـ ةـيـكـلـسـالـلـاـ ئـلـحـمـلـاـ ئـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ ئـدـحـوبـ ئـرـخـأـ ئـرـمـ ئـلـقـتـسـمـلـاـ (WLC)ـ نـمـ Ciscoـ.
عـداـخـمـ كـلـسـ	فـشـكـلـاـ مـتـ يـتـلـاـ تـاغـوارـمـلـاـ ئـاتـخـالـاـ اـهـنـيـكـمـتـ كـنكـمـيـ يـتـلـاـ رـايـتـخـالـاـ ئـنـاخـ قـأـعمـ ئـلـودـ رـيقـقـتـلـاـ .ايـئـاـقـلـتـ ئـيـكـلـسـلـاـ ئـكـبـشـلـاـ ئـلـعـ اـهـنـعـ.
SSIDـ مـادـخـتـسـاـ	نـعـ نـلـعـتـ يـتـلـاـ دـاغـوـأـلـاـ ئـاتـخـالـاـ اـهـنـيـكـمـتـ كـنكـمـيـ يـتـلـاـ رـايـتـخـالـاـ ئـنـاخـ ciscoـ لـاـ ،دـدـحـمـ رـيـغـ مـلـعـمـ اـذـهـ تـنـأـ كـرـتـيـ نـاـ .ايـئـاـقـلـتـ كـتـكـبـشـبـ صـاخـلـاـ قـأـعمـ ئـلـودـ رـيقـقـتـلـاـ .تـفـشـكـ قـرـامـ اـذـهـ اـمـدـنـعـ رـاـذـنـاـ دـلـيـ طـقـفـ.
ىـلـعـ حـلـاصـ لـيـمـعـ لـوصـوصـواـ ئـطـقـنـ ةـلـيـخـدـلـاـ	ةـطـقـنـ ئـلـعـ ايـئـاـقـلـتـ يـوـتـحـتـ ثـيـحـبـ اـهـنـيـكـمـتـ كـنكـمـيـ يـتـلـاـ رـايـتـخـالـاـ ئـنـاخـ رـيـغـ مـلـعـمـ اـذـهـ تـنـأـ كـرـتـيـ نـاـ .مـهـبـ قـوـثـومـ ئـالـمـعـ اـهـ بـ ئـنـرـتـقـمـ ئـلـيـخـدـ لـوصـوصـ ةـلـودـ رـيقـقـتـلـاـ .تـفـشـكـ قـرـامـ اـذـهـ اـمـدـنـعـ رـاـذـنـاـ دـلـيـ طـقـفـ ciscoـ WLCـ لـاـ ،دـدـحـمـ قـأـعمـ.
لـوصـوصـواـ ئـطـقـنـ ةـعـداـخـمـلـاـ ةـصـصـخـمـلـاـ	ايـئـاـقـلـتـ نـارـقـأـلـاـ تـاـكـبـشـ ئـاتـخـالـاـ اـهـنـيـكـمـتـ كـنكـمـيـ يـتـلـاـ رـايـتـخـالـاـ ئـنـاخـ رـيـغـ مـلـعـمـ اـذـهـ تـنـأـ كـرـتـيـ نـاـ .ةـطـسـاـوبـ اـهـنـعـ فـشـكـلـاـ مـتـ يـتـلـاـ رـيقـقـتـلـاـ .تـفـشـكـ ئـكـبـشـ اـذـهـ اـمـدـنـعـ رـاـذـنـاـ دـلـيـ طـقـفـ ciscoـ WLCـ لـاـ ،دـدـحـمـ قـأـعمـ ئـلـودـ.



ةيكلساللا ةيلحملاءكبسلا يف مكحتلارصنع لىاتانايبلالاسال قيبطت قوف رقنا  
هذه نيزخت متيو؛ ئقاط ١رود ربعتانايبلاب ئافتحالا متى ال نكلو، نم Cisco.  
ةرياطتملا يئاوشعلالوصولاركاذيف اتقؤم تاملعملما.

رمأولا رطس ئهجاو نم:

<#root>

(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

## ل ةيـسـاسـأـلـا ةـيـنـبـلـا عـمـ Prime

طاقن ورثكأ وأ دح او مكحت ةدحون يوكتل Cisco Prime ل ئيس اسألا ئينبلا مادختسا نكمي تاودأ ىلع Cisco نم (PI) ئادألا تامولعم ئينقت يوتحت. اهتبقارم و ئطبترمل (AP) لوصولا Cisco PI مدخلتسا امدنع . يف مكحتل او ريبكلا ماظنلا ئبقارم ليهستل Cisco لح يف طقون و ليمعلما يرود لكشب مكحتل اتادح و ددحت، يكلساللا ئدعاق يف عقاوملا نزختو (RFID) يكلساللا ددرتللا فرعم ئمالماع عقوم و ئليخدل لوصولا Cisco PI.

دع اوق مدخلت سرت و دع اوق ىل دن تسملا فى ينصلتla Cisco Prime ل ئيساسألا ئينبلا مع دت Cisco ىل تامىالملما مكحتلا ةدحو لسرت .مكحتلا ةدحو لىلع اهنىوكت مت يلتla فى ينصلتla Prime Infrastructure : ثادحألا هذه دع ب

- مكحتل زاهج لسري، ةرم لوأ ةقىدىصلالا ئلولودلا ئلإ فورعم رىغ لوص و ةطقن تلقتن ا اذا يىبنت ئللاح يف ةعداخملالا ئللاحلا تناناك اذا طقف Cisco Prime Infrastructure ئلإ ةديصم ئيجراخ وأ ئيلخاد ئيراحللا ئزوحلا تناناك اذا اخف لسري الو.
  - طاقن ئلإ ةديصم مكحتل زاهج لسري، ئلهملا ءاهتنان دعوب arogueentry ئلمازا تمت اذا ئيسياسألا ئينبلالا ئلإ لوصولا ئل ئيسبنت) ةفنسن رىغ وأ (ديدهت، ئيسبنت) ةراض اهنا ئىلع اهفييصنصت متى يتلا ئنمضملا : ئتقؤملالا نيزختلاب تادحومادختساب تالاخدالا هيجوت ئداعاب مكحتل ئدحوموقت ئيجراخل او ئيلخادل او ئقلعمل او.

## ةحصـلـا نـم قـقـحتـلـا

Monitor > روث علل ایل ایل علی افتلا ایص داخمل ایف دح و یف مکحت ایف هج اولا رسوس موس ایم، ئوقتانا لق.

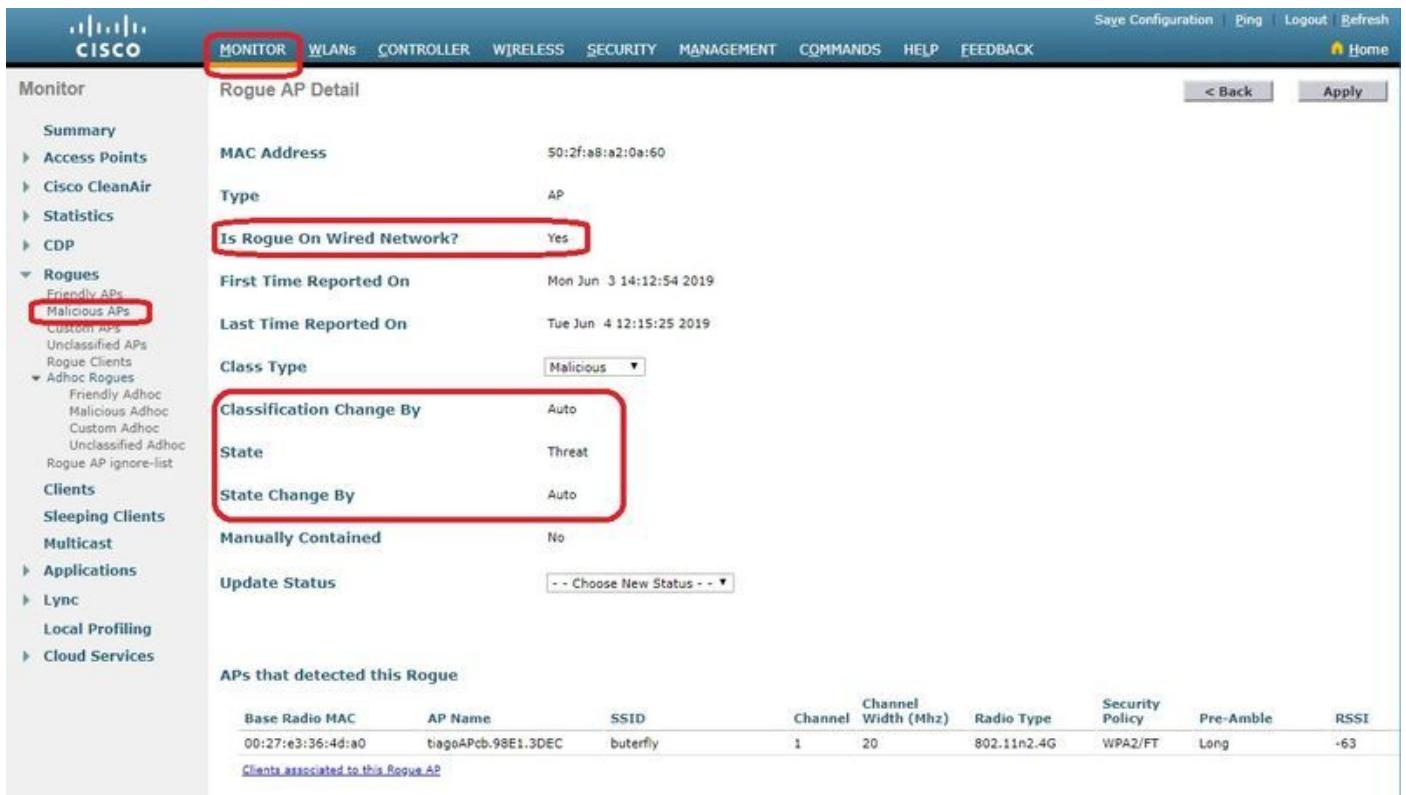
اطلس و لفظ خم فینصت رفوتوی، حفصلا هذه یف

- نم ۀقىدىصك اهيلع ۀمالماع عضومتى يتلا لوصولاطاقن - ۀفولأملالوصولاطاقن لوصولاللوق.

- طاقن وا RLDP رباع ئراض اهنأ ىلع اهفيروعت متي يتلا - ئراصلما (AP) لوصولما طاقن داخملما فشتكمىلل (AP) لوصولما.
- ئصصخم دعاوتك اهفينصت متي يتلا لوصولما طاقن - ئصصخملما لوصولما طاقن داخلم دعاوتك ئطس اوب.
- يضارف الكشب ئعداخملما لوصولما طاقن ضرع متي - ئفنصملا ريغ لوصولما طاقن مكحتلا ئدحو يف ئفنصم ريغ ئمىاقي.
- ئعداخملما لوصولما طاقنب نولصتم ئالمعلا - نوع داخملما ئالمعلا.
- نارقألا نوفيزملا ئالمعلا - داغوألا.
- ئالخ نم جردم وھ امك - ئعداخملما (AP) لوصولما طاقن لەاجت ئمىاقي PI.

 WLC نإف، اهسفن PI ئطس اوب ئلقتسملا لوصولما ئطقن و WLC ئرادا مت اذا: ئظحالم لوصولما طاقن لەاجت ئمىاقي يف هذه ئلقتسملا لوصولما ئطقن ايئاقلت درسي ئيلحملما ئكبشلا يف مكحتلا رصنع يف بولطم يفاضا نويوكت دجوي ال. ئعداخملما زىيملا هذه نيكىمتل (WLC) ئيكلساللا.

ىلع لاثم يلي امييف. ئقرايملا اذه لوح ليصافت ىلع لوصح لىل نيعم قرام لاخدا قوف رقنا: ئيكلسلا ئكبشلا ىلع هفاشتكا مت عداخم



The screenshot shows the Cisco WLC (Wireless Local Loop Controller) interface under the 'Monitor' tab. On the left, a navigation tree includes 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues' (selected), 'Clients', 'Sleeping Clients', 'Multicast', 'Applications', 'Lync', 'Local Profiling', and 'Cloud Services'. The main panel displays 'Rogue AP Detail' for a rogue access point with MAC address 50:2f:a8:a2:0a:60. Key fields shown include:

- Type:** AP
- Is Rogue On Wired Network?**: Yes (highlighted with a red box)
- 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 --

Below this, a table lists 'APs that detected this Rogue' with one entry:

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

A note at the bottom says: 'Clients associated to this Rogue AP'.

رماؤألا رطس ئهجاو نم:

<#root>

(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 Aps	#Rogue Clients	#Highest RSSI det-Ap	#RSSI	#Channel
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:a3:8e:db:01:b1	Unclassified Alert		2	0	00:27:e3:36:4d:a0 -28	40	
00:a3:8e:db:01:b2	Unclassified Alert		2	0	00:27:e3:36:4d:a0 -28	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

# اهالص او عاطخألا فاشكتسا

دغولا فاشتكا متي مل اذا

ةيـمـوسـرـلـا مـدـخـتـسـمـلـا ـهـجـاوـىـلـعـ .ـلـوـصـوـلـا ـهـطـقـنـىـلـعـ ـعـدـاخـمـلـا ـفـشـكـلـا ـنـيـكـمـتـ نـمـ قـقـحـتـ

The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes Save Configuration, Ping, Logout, Refresh, Home, MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar lists various wireless configurations under 'Wireless'. The main content area shows 'All APs > Details for tiagoAP.69F4.6458'. The 'Advanced' tab is selected. A red box highlights the 'Rogue Detection' checkbox under 'Data Encryption'. The right side of the screen displays several configuration sections: Power Over Ethernet Settings, AP Core Dump, AP Retransmit Config Parameters, VLAN Tagging, mDNS Configuration, TrustSec, and CMX Services.

رمـاـواـلـا رـطـسـهـجـاوـىـفـ:

<#root>

(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  
[...]
```

رملأا اذه مادختساب لوصولـة طقـنـىـلـعـعـداـخـمـلـاـفـشـكـلـاـنـيـكـمـتـنـكـمـيـ:

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

ىـلـعـدـمـتـعـتـوـطـقـفـDCAـدـلـبـلـاـتـاـونـقـحـسـمـبـيـلـحـمـلـاـعـضـوـلـاـنـمـلـوـصـوـلـاـةـطـقـنـمـوـقـتـ  
اـذـاـعـداـخـمـلـاـفـيـرـعـتـعـيـطـتـسـتـاـلـمـكـحـتـلـاـةـدـحـوـنـافـ،ـىـرـخـأـةـانـقـيـأـيـفـعـداـخـمـلـاـنـاـكـاـذـاـنـيـوـكـتـلـاـ  
نـمـقـقـحـتـلـلـرـمـأـلـاـاـذـهـرـدـصـأـ.ـةـكـبـشـلـاـيـفـةـبـقـارـمـلـاـعـضـوـيـفـلـوـصـوـطـاـقـنـكـيـدـلـنـكـيـمـلـ

```
<#root>  
(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
```

- ةـعـداـخـمـلـاـلـوـصـوـلـاـةـطـقـنـثـبـمـتـيـاـلـSSIDـ.
- وأـةـفـوـلـأـمـلـاـعـداـخـمـلـاـةـمـئـاـقـيـفـةـعـداـخـمـلـاـلـوـصـوـلـاـةـطـقـنـلـMـA~Cـنـاـونـعـةـفـاـضـاـمـدـعـنـمـدـكـأـتـ.  
ـلـالـخـنـمـهـجـارـدـابـحـوـمـسـمـهـنـأـPIـ.
- (AP) لـوـصـوـلـاـةـطـقـنـىـلـاـةـعـداـخـمـلـاـلـوـصـوـلـاـةـطـقـنـنـمـدـاشـرـالـاـةـزـهـجـأـىـلـاـلـوـصـوـلـاـنـكـمـيـاـلـيـتـلـاـمـزـحـلـاـطـاـقـتـلـاـلـالـخـنـمـعـاـجـإـلـاـاـذـهـنـمـقـقـحـتـلـاـنـكـمـيـ.ـعـداـخـمـدـوـجـوـنـعـتـفـشـكـيـتـلـاـفـشـتـكـمـجـلـاعـمـنـمـةـبـيـرـقـىـلـعـيـوـتـحـتـAPـ.
- فـاـشـتـكـاـلـقـئـاـقـدـ9ـىـلـاـلـصـيـاـمـقـرـغـتـسـتـنـأـيـلـحـمـلـاـعـضـوـلـاـيـفـلـوـصـوـلـاـةـطـقـنـلـنـكـمـيـ.

عداخمل (3 تارود 180x3).

- ئەمەلس لە ئانق لىثم تاددرت ىلۇغ تارىھلى فاشتىڭ Cisco نم لوصولا طاقنل نكىمىي ال (زىترەجىج 4.9 ئاماعلا).
- فېط) FHSS ىلۇغ لەمعت يېتلى داغۇلما فاشتىڭ Cisco نم لوصولا طاقنل نكىمىي ال (تاددرتلى يەطخت راشتنالا).

## ۋەدىفەملە ئاطخالا حىحصىت

<#root>

(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
*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 -64
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestamp set to 1595724417. Detecting
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 SYNC for Channel (new/old : 1/0) or channel will
*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,
*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 1radInfo->containSlotId = 2 Received
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malicious
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule classification :
*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
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*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
*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: buterfly
```

<#root>

```
(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 :FCW22
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for proces
*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTi
*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
*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
*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
*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
*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
*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
*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 timestamp expired. last update at 0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: knownApCount=0, totalNumOfRogueE
*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
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: avgNumOfRogues[0]/10=4, rogueAla
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestamp expired. last update at 0
*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 w
*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,
*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,
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclass
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xffff
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for : Class Change by
*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
*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
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclass
*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
*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:
*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 Modifi
*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
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 Receiv
*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
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for : Class Change by
```

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Send Rogue Info Notificaiton for AP report 00:  
\*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  
\*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

\*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,  
\*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 Receiving  
\*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 unclassified

\*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

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot apply rule

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification : Class unclassified

\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1

\*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

\*apfRogueTask\_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7

\*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

\*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 -59  
\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecting  
\*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 -59  
\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 SYNC for Channel (new/old : 40/0) or channel width  
\*apfRogueTask\_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecting  
\*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  
\*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, mode  
\*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, mode  
\*apfRogueTask\_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1 Receiving  
\*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 lradInfo->containSlotId = 2 Receiving  
\*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  
\*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=bliz
*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
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but
*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
*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 Imp
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*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 Imp
*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: butterfly
*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
*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
*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
*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: butterfly
*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
*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
*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
*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
*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 0xffff0000
*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
```

## دحأ ئەلزا/فاشتكا درجمب نىع داخملار ئەمئاقلا نم:

0	، ويئوي 5 جوزتم 09:01:57:2019	لوصو ئەطقن 1 ئەطس اوب b4:c0:f5:2b:4f:90 فاشتكا مти: ع داخملار لىيمعلار فشك رخآ، هېبنت: ئەلچىلار BSSID: a6:b1:e9:f0:e8:41، ع داخلمىرىم (APs) mac ع داخلمىرىم ئەب اوب 00:27:e3:36:4d:a0: لوصولار ئەطقنلار 00:00:00:02:02:02.
1	5 يف جوزتم 09:00:39: ويئوي 2019	زاهج نم اهتلارا تىمت يىتلا 9c:97:26:61:d2:79: ئەع داخملار لوصولار ئەطقن يىس اسالا ويىدارلا ربع (MAC) طىاسوللار لوصولار يف مكحتلا 00:27:e3:36:4d:a0: no:0(802.11n(2.4) (زترهاجيچ
2	، ويئوي 5 جوزتم 5:53:39 م 2019 م	زاهج نم اهتلارا تىمت يىتلا 7c:b7:33:c0:51:14: ئەلچىلار لوصولار ئەطقن يىس اسالا ويىدارلا ربع (MAC) طىاسوللار لوصولار يف مكحتلا 00:27:e3:36:4d:a0: no:0(802.11n(2.4) (زترهاجيچ
3	، ويئوي 5 جوزتم 5:52:27:2019 م	لوصو ئەطقن 1 ئەطس اوب FC:3f:7c:5f:b1:1b فاشتكا متي: ع داخملار لىيمعلار فاشتكا رخآ، هېبنت: ئەلچىلار BSSID: 50:2f:a8:a2:0a:60، ع داخلمىرىم (APs) mac ئەع داخلمىرىم ئەب اوب 00:27:e3:36:4d:a0: لوصولار ئەطقنلار 00:26:44:73:c5:1d.
4	، ويئوي 5 جوزتم 5:52:17:2019 م	زاهج نم اهتلارا تىمت يىتلا D4:28:d5:da:e0:d4: ئەلچىلار لوصولار ئەطقن ئىكلساللا طىاسوللار لوصولار يف مكحتلا 00:27:e3:36:4d:a0: no:0(802.11n(2.4) (زترهاجيچ يىس اسالا

## تايصوت

يىف ئەلمىتحم ع داخلمىرىم دوجو يىف كىشت تىنك اذى تاونقىلا ع يىمجىلى ئانقلارا صحف نىيوكىت بىمق كىتابش.

لكل دحاؤنم اھع قوم و ع داخملار فشك ئەزىجىپ ئەصاخلى لوصولار طاقىن ددع فلتتىي نأ نكىمىي 2. نم . ئىكلسلى ئەكبىشلى طىيەتلىك كىلدىق قوقۇتىي، ئىنبىم لكل دحاؤلى قباط نم قباطلىك يف لقألا ئىلۇم دحاؤم داخلمىرىم ئەطقن ئەننە نوکىي نأ نسەحتسىملا ئەكبىش ثې تالاجم ع يىمجىل لاصقىتا طاخ بىلەتت ئەع داخملار لوصولار ئەطقن نأ. ئىنبىملا ئەكبىشلى يقىطنىملا طىيەتلىك دەمەتىعىي ع ضولار نإف، اهتبقارم بىجي يىتلا 2 ئەقبطىلا.

## فەنصىم رىغ دوغولار ناك اذى

حىيىص لىكشىب ئەع داخملار دعاوچىلا نىيوكىت نم قىقىخت

ۋەدىفەملار ئاطاخالا حىيىصىت

<#root>

(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 :FCW2245M0

```
(Cisco Controller) >
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLr
*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, maxRssiLr
*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRule

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

## تايصوت

نيكمتب مق وأفولأمل اقمىاقلا يف اهفصأف، فورعم ظعداخم تالاخدا كيدل تنناك اذا تالاخدا دوجونم دكأتو (AAA) ةبساحمل او ضيوفتل او ئقاداصمل مادختساب ئحصىلا نم ققحتلا ةبساحمل او ضيوفتل او ئقاداصمل تاناييب ئداعاق يف فورعملا ليمعلا (AAA).

## داغوألا عقوم ددحي ال RLDP جمانرب نا

- لمعي ال RLDP ناف، ئانق يف دغولنا ناك اذا.
- وحوتفرم ظعداخمل (WLAN) ئيكليساللا ئيلحمل اكبسشلا ئكبشلا تتنناك اذا طقف RLDP لمعي ارفوتمناكو.
- كراشت ال اهناف، ئانق يف ليمعلا مدخلت يلحمل اعضولنا نم لوصولنا ئطقىن تتنناك اذا ئيلمع يف RLDP.
- و 1800i و 1810 OEAP و 3800 Series AP، 1810W و 1815 و 1830 و 1850 و 2800 و 3800.

## ةديفمل اءاطخألا حيحصت

```
<#root>
```

```
(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

\*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 = 100

\*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: 0xffffd682b5b8, 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!!!! msrb 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 Started

\*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 Started

\*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
```

## تايصوت

1. ايدبطة قيبط رلدى ايلع داخملات الا خدا.

2. يرود لكشب رلدو.

3. ئابسنلاپ. ئابقارملا عضوأ ئيلحملات (APs) لوصول ا طاقن ئيلع RLDP رشن نكمي، ئالى عالمي ئامد ئيلع ريشأت يأ ئيلع ئاضقلى، ئايوطتلل ئيلباق رثكألا رشنلا تايىلمعل، كلذ عم و ناكما لا دنع ئابقارملا عضويف لوصول ا طاقن ئيلع RLDP ئينقت رشن متى، ئابقارملا عضول (AP) لوصو ئاطقنى ئيشغت رشن متى نأ ئيصوتلا هذه بلى طتت يف لوصو ئاطقنى 5 لكل ضرعلا زاهج عضول ئادحاو لوصو ئاطقنى لثم ئيجذومن ئابسنلا ضرعلا زاهج عضويف (APs) لوصول ا طاقن نم ئادفاتسالا نكمي امك. ئيلحملات عضول ا فەمملا هذهل فيكتلل لباقلات wIPS زارت.

## داخملات فشك لوصول ا ئاطقنى

مكحت ئادحو يف رمألا اذه مادختساب داخملات فشك زاهج يف داخملات الا خدا ئيؤرنكمي، ئالاحلا نيءيعت ئيلا ئامالعلان لقتنت، نيءيكلسلا نيءيعداخملل ئابسنلاپ.

```
<#root>
tiagoAP.6d09.eff0#
show capwap rm rogue detecto
r
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

```

لوصول ا ظقون مكحت ةدحو يف ةديفمل ا عاطخألا حيحةصت رم اوأ (AP)

<#root>

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 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*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.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e

```

نـيـعـداـخـمـلـاـعـاوـتـحـاـ

عـقـوـتـمـلـاـعـاطـخـأـلاـحـيـحـصـتـ

```
<#root>
```

```
*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, slotid 1
*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 list
*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
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6 ContainmentLevel = 6

*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 Received from AP

*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 : 0

*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 1

*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
*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 to -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 = -31 to -33
*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 to -36
*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
*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
*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
*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
*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
```

## تايصوت

قرم لك يف ڙهنجا 3 ىلع Flex-Connect/يچمل اعضوا نم لوصولا ڦطقني یوتحت نأ نكمي. لکل ڙهنجا 6 ىلع ڦاشلا عضونم لوصولا ڦطقني یوتحت نأ نكمي، يکلسال زاهج لکل دھلا ىلع لعفلاب یوتحت ال لوصولا ڦطقني نأ نم دکأت، کل ذل ڙجيتنو. يکلسال زاهج قيلعات ڦلاح يف ليمعلا نوكني، ويرانيسلا اذه يف. اه بحومس ملا ڙهنجا ددععل یصقا لآ عاوتحا لآ.

يئاقلتلا ئاوتحالا دعاوقة نم ققحتلا 2.

راقرد

وهي تدعى Cisco، وهي مكونة من مكونات مثل المراقبة، التحليل، التعلم الآلي، والذكاء الاصطناعي، مما يسمح لها بفهم وتحليل البيانات بشكل عميق ومتعدد الأبعاد.

ةلص تاذ تامولع

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).