Overzicht op 802.11h, TPC-regeling (Transmission Power Control) en selectie van dynamische frequenties

Inhoud

Inleiding

Dit document geeft een overzicht van het onderdeel draadloze 802.11-standaard: 802.11u en de impact van dit amendement op draadloze implementaties en wat het vertaalt in configuratie. Dit amendement had twee hoofdpunten: Dynamic Frequency Selection (DFS) en Transmit Power Control (TPC). DFS, als spectrumbeheer (hoofdzakelijk om samen te werken met radars) en TPC, om de totale RF-"vervuiling" van draadloze apparatuur te beperken.

Voorwaarden

Vereisten

Voor dit document is alleen een zeer eenvoudig begrip van Wi-Fi- of 802.11-protocol vereist. De nadruk ligt echter op specifieke kwesties van outdoorimplementaties en zal beter worden begrepen met een kleine Wi-Fi-implementatieervaring.

Gebruikte componenten

Een Cisco Wireless LAN Controller (WLC) op 8.0-software wordt alleen gebruikt voor referentie van de configuratie.

DFS

DFS gaat allemaal over radardetectie en -vermijding. Radar staat voor "radiodetectie en -bereik". In het verleden gebruikten de radars om te werken in frequentiebereik waar zij het enige type toestel waren dat daar actief was. Nu de regelgevende instanties deze frequenties voor ander

gebruik (zoals draadloos LAN) openen, is er een behoefte aan deze apparaten om in overeenstemming met de radars te functioneren.

Het algemene gedrag van een apparaat dat voldoet aan het DFS-protocol is dat hij kan detecteren wanneer een radar in het kanaal zit, dat bezette kanaal niet meer gebruikt, een ander kanaal bewaakt en er op springen als dat duidelijk is. (dat wil zeggen dat er ook geen radar is).

Het proces voor een radio om een radar te detecteren is een ingewikkelde taak die eigenlijk geen deel uitmaakt van de standaard. Er kunnen dus foute radardetecties optreden en dat is een kunst die het Wi-Fi-verkoopalgoritme combineert met de Wi-Fi-chips. De detectie zelf is echter verplicht door het regelgevende agentschap en is duidelijk omschreven. Daarom zijn scanparameters niet configureerbaar.

In een vroeg stadium was DFS vereist voor ETSI-apparatuur (European Telecommunication Standard Institute) die in de Europese Unie (en landen die de ETSI-regelgeving volgen) in de ETSI 5ghz-band werkt. Het is niet noodzakelijk verplicht in andere delen van de wereld en hangt ook af van het frequentiebereik. De Amerikaanse Federal Communication Commission (FCC) heeft deze nu verplicht gemaakt voor UNII-2 en UNII-2 uitgebreid frequentiebereik zoals ETSI.

DFS-bewerkingen maken gebruik van verschillende manieren om informatie tussen stations uit te wisselen. Informatie kan in specifieke elementen in het baken- of testantwoord worden opgenomen, maar een specifiek kader kan ook worden gebruikt om informatie te rapporteren: het actiekader. Wij zullen dat invoeren nadat wij hebben uitgelegd wanneer zij van start gaan.

Meer informatie over radars

Radars kunnen worden vastgesteld (vaak civiele luchthaven- of militaire basis, maar ook weerradar) of mobiel (schepen). Een radarstation zal een reeks krachtige pulsen periodiek verzenden en de reflecties waarnemen. Omdat de energie die teruggaat naar de radar veel zwakker is dan het oorspronkelijke signaal, moet de radar een zeer krachtig signaal uitzenden. Omdat de energie die terugkomt op de radar zeer zwak is, kan deze ook verwarren met andere radiosignalen (zoals een draadloos LAN om een voorbeeld te geven).

Omdat de 2,4 GHz-band vrij is van radar, zijn de DFS-regels alleen van toepassing op de 5,250-5,725 GHz-band.

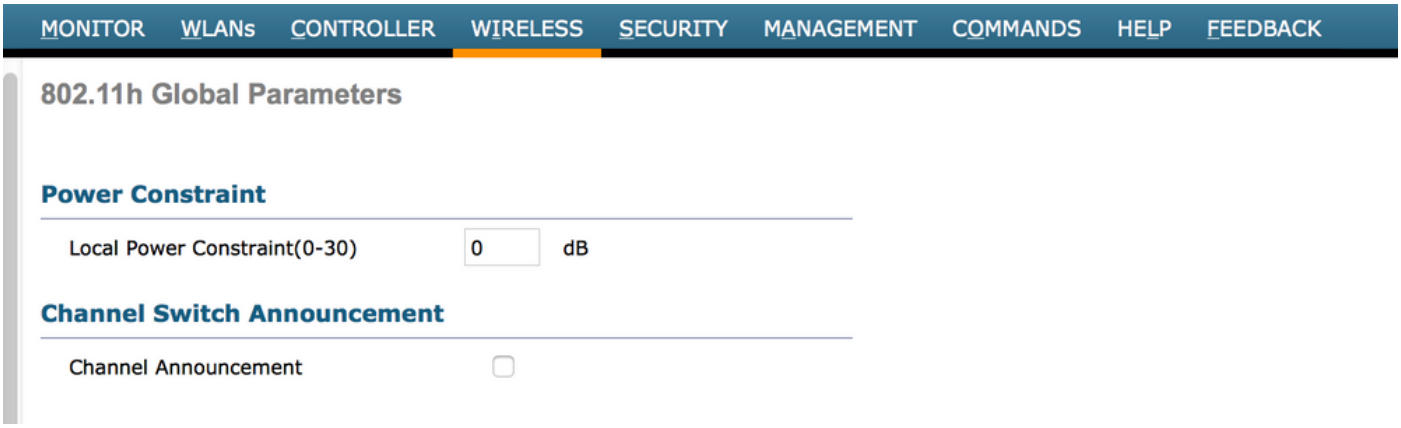
Wanneer de radio een radar detecteert, moet zij het gebruik van het kanaal tenminste 30 minuten stopzetten om die dienst te beschermen. Hij volgt dan een ander kanaal en kan het na ten minste 1 minuut gebruiken als er geen radar is gedetecteerd.

Het volgende onderwerp is meer verwant aan het oplossen van problemen in een milieu van Cisco in plaats van uitleg over de standaard. Sommige punten kunnen echter voor iedereen interessant zijn en zijn kort genoeg om hieronder kort te worden toegelicht.

DFS-in Cisco WLC

DFS is vaak gekoppeld aan mesh, maar is eenvoudigweg gerelateerd aan outdoorgebieden (of zelfs binnengebieden die outdoorsignalen horen en werken op binnen-/outdoorkanalen). Als een AP een radar hoort, zal het kanaal veranderen en het vorige kanaal 30 minuten verbieden. Dit is nogal ruw voor klanten. "Kanaalaankondiging" is een mooi kenmerk waarbij het AP de klant vertelt dat het dit kanaal uitsluit en naar welk kanaal het nu gaat.

Tenzij u een dual-backhaul gebruikt, werken al uw Root mesh AP's (RAP's) en mesh kind AP's (MAP's) op hetzelfde kanaal. Het kan dus gebeuren dat alleen een MAP de radar detecteert. Dan is het de enige die kanaal wijzigt en is het niet beschikbaar om minstens 30 minuten met de andere AP's te praten (de tijd om terug te keren op dit kanaal). Als je wilt dat je hele backhaul beweegt zodra een AP een radar detecteert, dan kan je de "kanaalaankondiging" functie inschakelen en zal het AP dat de radar detecteert de anderen (inclusief de RAP) vertellen voordat ze van kanaal veranderen zodat ze allemaal samen bewegen. Daarna scannen ze allemaal een ander kanaal gedurende één minuut, dat de stille periode wordt genoemd. Dit is om ervoor te zorgen dat het nieuwe kanaal ook geen radar bevat.



Dit menu is beschikbaar in Wireless-N>802.11a-8DFS in de webinterface van de WLC

Gevolgen van DFS-regels

AP moet bij het bewegen naar een nieuw DFS kanaal één minuut lang stilletjes naar het medium luisteren voordat het iets mag verzenden (zoals een baken) om er zeker van te zijn dat er momenteel geen radar actief is op dat kanaal. Clients hebben niet zo'n verantwoordelijkheid en mogen Wi-Fi-frames verzenden als er al een AP op het kanaal aanwezig is en actief is, hetgeen alle verantwoordelijkheid laat

Op de schouders van het AP. Bepaalde kanalen zoals 120,124 en 128 hebben specifieke regels waarbij een AP zelfs 10 minuten moet wachten voordat hij die kanalen kan gebruiken.

Dit betekent dat klanten, wanneer ze naar een DFS-kanaal verhuizen, doorgaans meer dan 100 ms moeten wachten om een baken te kunnen horen. Dit betekent dat de scaninspanning zeer kostbaar is, aangezien de klant geen verzoeken om onderzoek op een nieuw kanaal mag sturen en op een baken moet wachten. Veel verkopers van Wi-Fi-apparaten van klanten kennen dit en ontprioriteren DFS-kanalen in hun roaming-/scanalgoritme. Clients scannen geen DFS-kanalen zeer vaak vanwege de kosten van het doen daarvan.

Onjuiste radardetectie

Er is een delicaat evenwicht tussen gevoelig zijn om te voldoen aan DFS-vereisten (detecteren van radars) en niet te gevoelig zijn om foutieve detectie te voorkomen. De meest voorkomende oorzaak van onjuiste detectie is, om kostenredenen, het plaatsen van een andere AP samen gevestigd (op dezelfde pool bijvoorbeeld). Zelfs als die AP een ander kanaal gebruikt, als dat kanaal dicht is, kan een puls van buiten band voor deze andere AP voorkomen maar zal worden gezien als in-band pulsen en verkeerd als radar worden genomen. De beste oplossing is zorgvuldige kanaalplanning en AP plaatsing.

Een andere oorzaak is een radar die een vuil off-kanaal signaaloverdracht heeft of zo krachtig op zijn kanaal is dat hij zijdelingse transmissie heeft op aangrenzende kanalen. Dus zelfs als het AP op het kanaal naast de radar staat, stuurt de radar een aantal nevensignalen op het AP-kanaal waardoor de AP gelooft dat een radar op het kanaal werkt, hoewel het dat niet is. De oplossing hier is nog om AP kanaal en AP plaatsing te veranderen.

Onlangs werd ook gezien dat sommige legitieme apparaten van derden (of klanten) hun Wi-Fi-chipset hadden die soms pulsen verzenden die op radarsignalen lijken. Het is een contant fijnafstemming om ervoor te zorgen dat het DFS-algoritme alleen echte radars laat zien. Het kan de moeite waard zijn om vrij te geven notities voor bug ids te controleren met betrekking tot verbeteringen van het DFS-algoritme.

Cisco AP's die een Cleanair of Rf ASIC chip hebben kunnen deze spectrumanalyzer gebruiken om raders met een veel accuratere nauwkeurigheid te detecteren. Zij zullen doorgaans een veel minder valse positieve signalering hebben, aangezien zowel de wifi-chip als de Cleanair/RF ASIC-chip de signalen zal analyseren en een radargebeurtenis alleen zal plaatsvinden als beide overeenkomen dat het van een radar gehoord signaal afkomstig is. Hierdoor kan een mate van nauwkeurigheid worden bereikt die niet kan worden bereikt door radio-AP's die alleen WiFi gebruiken.

Debugs

U vindt voornamelijk DFS-gebeurtenissen met traplogs, maar alternatieven zijn:

```
show int d1 dfs  (on AP)
show mesh dfs h  (on AP)
```

AP zal die onthouden tot de volgende herstart.

Klanten die in de EU of in regio's met soortgelijke regelgeving buitenshuis AP’s inzetten, moeten deze optie mogelijk maken.
>CONVERSIE GEÏNTEGREERD 802.11a-kanaalplatform voor buitengebruik

Als de enabled-controller geen controle uitvoert voor niet-DFS-kanalen in de DCA-lijst. De standaard status is uit (bestaand gedrag).

Meer informatie over CSCsl90630.

TPC vs DTPC vs Wereldmode

Heb je al eens gehoord over TPC (Transmission Power Control), DTPC (Dynamic Transmit Power Control) en World Mode? Ze zien er hetzelfde uit, maar doen niet echt dezelfde dingen... Laten we ze allemaal snel bekijken:

- De **Wereldmodus** is waarschijnlijk de oudste. Het is 802.11d wijziging van het Wi-Fi-protocol. Het is een functie die u kunt configureren op de Autonome (aIOS) access points en die standaard ingeschakeld is op lichtgewicht AP's en waardoor een client in World Mode zijn radiofarameters van het access point ontvangt. Paramters zijn feitelijk kanalen en energieniveaus. Maar neem het

niet verkeerd op. "Kanalen" heeft een "S". Het is niet het kanaal waarop de klant moet zijn! Om het toegangspunt te kunnen horen, moet de klant toch op het juiste kanaal staan. De Wereldmodus gaat dus over "de lijst met toegestane kanalen in dit land" en "de machtsniveaus zijn toegestaan in dit land".

-**TPC, Transmit Power Control**, is in feite een functie van 802.11h samen met DFS, waarmee het access point lokale regels voor de maximale transmissie kracht kan definiëren. Er zijn veel redenen waarom dit zou worden gebruikt. Je zou kunnen zijn dat de beheerder een andere reeks regels wil instellen dan het maximum van het regelgevende domein vanwege specifiekere lokale regels of omgeving. Een andere mogelijkheid is dat de beheerder weet dat het een zeer dichte WiFi-implementatie is met een intense dekking: Daarom zetten AP's zich in op een lager transmissievermogen (dankzij het RRM-algoritme) en TPC is een statische manier om klanten te dwingen ook hun vermogen te verlagen en dus hun dekking te verlagen zodat ze niet de buurlanden/AP's verstoren die op hetzelfde kanaal staan.

-**DTPC, dat is Dynamic Transmit Power Control**, lijkt dicht bij TPC maar heeft geen direct verband. Het is een eigen Cisco-systeem. Met DTPC zendt uw Cisco access point informatie over welke energieniveau u wilt gebruiken naar uw Cisco CCX-conforme klanten.

Ja, het ligt dicht bij de twee andere protocollen die hierboven zijn toegelicht... DTPC zal echter dynamisch zijn naarmate de client zich dichter of verder van de AP beweegt. Als uw client CCX is, kunt u daadwerkelijk meer doen: beïnvloeden. Zeer vaak heeft de AP een goede 9 dBi-patchantenne en de client heeft een slechte rubberen eend van 2,2 dBi antenne. Uw client hoort de AP goed, maar het clientsignaal gaat verloren in de omringende ruis en uw AP hoort het niet goed (ondanks de antenneversterking verbetert ook het ontvangen signaal). Uw cliënt zou zijn vermogensniveau moeten verhogen, maar het weet niet dat AP het niet goed hoort... het enige dat het weet is dat het (de cliënt) het AP goed hoort en van dit ontvangen signaal zijn eigen vermogensniveau aftrekt. Als je cliënt CCX is, kan AP de klant vertellen: "Ik hoor je niet goed, vergroot je macht tot 20 mW", of "ze hoeven niet te schreeuwen! uw stroom terug te brengen naar 5 mW, waardoor uw batterij zal worden gered." In deze informatie kan AP maximum overbrengen ("verhoog uw macht opnieuw, maar ga niet verder dan 50 mW").