Übersicht über 802.11h, Transmit Power Control (TPC) und Dynamic Frequency Selection

Inhalt

Einleitung

Dieses Dokument bietet eine Übersicht über einen Teil des Wireless-Standards 802.11: 802.11h und die Auswirkungen dieses Änderungsantrags auf Wireless-Bereitstellungen und dessen Auswirkungen auf die Konfiguration. Dieser Änderungsantrag sollte zwei Hauptaspekte enthalten: Dynamic Frequency Selection (DFS) und Transmit Power Control (TPC). DFS, als Spektrum-Management (hauptsächlich für die Zusammenarbeit mit Radargeräten) und TPC, zur Begrenzung der allgemeinen "Funkbelastung" von Wireless-Geräten.

Voraussetzungen

Anforderungen

Dieses Dokument erfordert nur ein sehr grundlegendes Verständnis des Wi-Fi- oder 802.11-Protokolls. Der Schwerpunkt liegt jedoch auf spezifischen Problemen bei der Bereitstellung im Außenbereich. Durch die Implementierung eines kleinen Wi-Fi-Netzwerks wird das Verständnis verbessert.

Verwendete Komponenten

Ein Cisco Wireless LAN Controller (WLC) für die Software 8.0 wird nur als Konfigurationsreferenz verwendet.

DFS

Bei DFS dreht sich alles um Radarerkennung und -vermeidung. Radar steht für "Radio Detection and Ranging". In der Vergangenheit wurden Radare in Frequenzbereichen eingesetzt, in denen sie die einzige Art von Gerät waren, die dort betrieben wurde. Jetzt, da Regulierungsbehörden diese Frequenzen für andere Zwecke (z. B. für Wireless LAN) öffnen,

müssen diese Geräte entsprechend der Radarwerte betrieben werden.

Das allgemeine Verhalten eines Gerätes, das dem DFS-Protokoll entspricht, soll erkennen können, wenn ein Radar den Kanal belegt, dann die Nutzung des besetzten Kanals beenden, einen anderen Kanal überwachen und auf ihn springen, wenn er klar ist. (d. h. dort auch kein Radar).

Der Prozess zur Erkennung eines Radars ist eine komplizierte Aufgabe, die eigentlich nicht zum Standard gehört. Daher kann es zu falschen Radarerkennungen kommen, die den Algorithmus des Wi-Fi-Anbieters mit den Wi-Fi-Chip-Funktionen kombinieren. Die Erkennung selbst ist jedoch von der Regulierungsbehörde vorgeschrieben und klar definiert. Die Scanparameter sind daher nicht konfigurierbar.

Im ETSI 5ghz-Band war bereits früh DFS für Geräte des European Telecommunication Standard Institute (ETSI) erforderlich, die in der Europäischen Union (und in Ländern, die ETSI-Vorschriften einhalten) arbeiten. Sie ist nicht unbedingt in anderen Teilen der Welt obligatorisch und hängt auch vom Frequenzbereich ab. Die American Federal Communication Commission (FCC) hat den erweiterten Frequenzbereich UNII-2 und UNII-2 wie ETSI jetzt zwingend vorgeschrieben.

Für DFS-Operationen werden verschiedene Möglichkeiten zum Informationsaustausch zwischen Stationen verwendet. Informationen können in bestimmte Elemente der Beacon- oder Sonde-Antwort eingegeben werden, aber auch ein bestimmter Frame kann zur Meldung von Informationen verwendet werden: Aktionsrahmen. Wir werden dies einführen, nachdem wir erklären, wann sie ins Spiel kommen.

Weitere Informationen zu Radaren

Radare können fest (oft zivile Flughäfen oder Militärstützpunkte, aber auch Wetterradar) oder mobil (Schiffe) sein. Eine Radarstation sendet regelmäßig eine Reihe von starken Impulsen und beobachtet die Reflexionen. Da die auf das Radar reflektierte Energie viel schwächer ist als das ursprüngliche Signal, muss das Radar ein sehr starkes Signal übertragen. Da die im Radar reflektierte Energie zudem sehr schwach ist, kann sie mit anderen Funksignalen verwechselt werden (z. B. mit einem WLAN).

Da das 2,4-GHz-Band frei von Radar ist, gelten die DFS-Regeln nur für das 5,250-5,725-GHz-Band.

Wenn das Funkmodul ein Radar erkennt, muss es mindestens 30 Minuten lang aufhören, den Kanal zu nutzen, um diesen Dienst zu schützen. Er überwacht dann einen anderen Kanal und kann diesen nach mindestens einer Minute wieder verwenden, wenn kein Radar erkannt wurde.

Das folgende Thema bezieht sich eher auf die Fehlerbehebung in einer Cisco Umgebung als auf die Erläuterung des Standards. Einige Punkte können jedoch für alle von Interesse sein und sind kurz genug, um hier kurz erläutert zu werden.

DFS in Cisco WLC

DFS ist oft mit Mesh verbunden, bezieht sich jedoch nur auf Außenbereiche (oder sogar Innenbereiche, die Außensignale hören und auf Innen-/Außenkanälen arbeiten). Wenn ein AP ein Radar hört, wechselt er den Kanal und untersagt den vorherigen Kanal für 30 Minuten. Das ist ziemlich unhöflich gegenüber den Kunden. "Channel-Ankündigung" ist eine nützliche Funktion,

bei der der Access Point dem Client mitteilt, dass er diesen Kanal ausschließt und in Richtung dessen Kanal sich dieser nun bewegt.

Wenn Sie kein Dual-Backhaul verwenden, werden alle Root Mesh APs (RAPs) und Mesh Child APs (MAPs) auf demselben Kanal betrieben. So kann es passieren, dass nur ein MAP das Radar erkennt. Es ist dann der einzige Kanal, der den Kanal wechselt, und es ist nicht möglich, mindestens 30 Minuten mit den anderen APs zu sprechen (der Zeitpunkt, zu dem dieser Kanal wiederhergestellt werden soll). Wenn Sie möchten, dass sich Ihr gesamtes Backhaul bewegt, sobald ein AP ein Radar entdeckt, können Sie die Funktion "Kanalankündigung" aktivieren, und der AP, der das Radar erkennt, teilt dies den anderen (einschließlich des RAP) mit, bevor Sie den Kanal wechseln, sodass sich alle zusammen bewegen. Sie scannen dann alle einen anderen Kanal für eine Minute, die als ruhige Phase bezeichnet wird. Damit soll sichergestellt werden, dass der neue Kanal auch kein Radar enthält.

Dieses Menü ist in Wireless->802.11a->DFS in der Webschnittstelle des WLC verfügbar.

Falsche Radarerkennung

Es besteht ein heikles Gleichgewicht zwischen der Fähigkeit, sensibel genug zu sein, um die DFS-Anforderungen zu erfüllen (Erkennung von Radaren), und der Unempfindlichkeit, um Fehlerkennung zu vermeiden. Die häufigste Ursache für eine fehlerhafte Erkennung besteht darin, aus Kostengründen einen anderen Access Point am gleichen Einsatzort einzusetzen (z. B. am gleichen Mast). Selbst wenn dieser AP einen anderen Kanal verwendet, kann ein solcher Impuls, falls dieser Kanal nahe ist, für diesen anderen Access Point ein Off-Band-Signal auslösen, jedoch als In-Band-Impulse angesehen und fälschlicherweise als Radar angesehen werden. Die beste Lösung ist eine sorgfältige Kanalplanung und AP-Platzierung.

Eine weitere Ursache ist ein Radar, das eine schmutzige Off-Channel-Signalübertragung hat oder auf seinem Kanal so leistungsstark ist, dass es eine Sideband-Übertragung auf benachbarten Kanälen hat. Auch wenn sich der Access Point auf dem Kanal neben dem Radar befindet, sendet das Radar einige Seitensignale auf dem AP-Kanal, wodurch der Access Point glaubt, dass ein Radar auf dem Kanal funktioniert, obwohl dies nicht der Fall ist. Die Lösung besteht weiterhin darin, die Platzierung von AP-Kanälen und APs zu ändern.

In letzter Zeit wurde auch festgestellt, dass einige legitime Geräte (oder Clients) von Drittanbietern ihren Wi-Fi-Chipsatz hatten, der manchmal Impulse sendete, die wie Radarsignale aussahen. Es ist eine kontinuierliche Feinabstimmung, um sicherzustellen, dass der DFS-Algorithmus nur echte Radare erkennt. Es kann sich lohnen, die Versionshinweise auf Bug-IDs hinsichtlich der Verbesserungen des DFS-Algorithmus zu überprüfen.

Debugger

Sie erkennen hauptsächlich DFS-Ereignisse mit Traplogs, aber es gibt Alternativen:

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

Der Access Point wird sich diese bis zum nächsten Neustart merken.

Kunden, die APs für Außenbereiche in der EU oder Regionen mit ähnlichen Vorschriften bereitstellen, sollten diese Option aktivieren.
>erweiterte Konfiguration 802.11a-Kanal für Outdoor-ap-dca aktivieren

Wenn der Controller aktiviert ist, führt er keine Prüfung auf Nicht-DFS-Kanäle in der DCA-Liste durch. Der Standardstatus lautet Off (vorhandenes Verhalten).

Weitere Informationen zu CSCsl90630.

TPC vs. DTPC vs. World-Modus

Haben Sie schon von TPC (Transmit Power Control), DTPC (Dynamic Transmit Power Control) und World Mode gehört? Sie sehen gleich aus, machen aber eigentlich nicht dasselbe.. Sehen wir uns die folgenden Punkte kurz an:

- **World Mode** ist wahrscheinlich der älteste. Es handelt sich um eine 802.11d-Änderung des Wi-Fi-Protokolls. Diese Funktion können Sie auf den autonomen Access Points (aIOS) konfigurieren, die standardmäßig auf leichten Access Points aktiviert ist und über die ein Client im World Mode seine Funkparameter vom Access Point empfängt. Parameter sind Kanäle und Leistungsstufen. Aber nehmen Sie es nicht falsch. "Channels" hat ein "s". Es ist nicht der Kanal, auf dem der Client sein sollte ! Um den Access Point zu hören, muss sich der Client trotzdem auf dem richtigen Kanal befinden. Worum es im World Mode also geht, ist "die Liste der zulässigen Kanäle in diesem Land" und "die Leistungsstufen sind in diesem Land zulässig".

-**TPC, Transmit Power Control**, ist eine Funktion von 802.11h zusammen mit DFS, mit der der Access Point lokale Regeln für maximale Übertragungsleistung definieren kann. Es gibt viele Gründe, warum dies verwendet wird. Eine davon könnte sein, dass der Administrator aufgrund speziellerer lokaler Regeln oder Umgebungen einen anderen Satz von Regeln festlegen möchte als die maximal zulässige regulatorische Domäne. Ein weiterer könnte sein, dass der Administrator weiß, dass es sich um eine sehr dichte Wi-Fi-Bereitstellung mit intensiver Abdeckung handelt: Daher stellen sich die Access Points auf eine niedrigere Übertragungsleistung ein (dank des RRM-Algorithmus), und TPC ist eine statische Methode, um Clients zu zwingen, auch ihre Leistung zu senken und somit ihre Abdeckung zu verringern, sodass sie nicht Nachbarclients/APs stören, die sich auf demselben Kanal befinden.

-**DTPC, das ist Dynamic Transmit Power Control**, sieht nahe an TPC, hat aber keine direkte Beziehung. Es ist ein proprietäres System von Cisco. Mit DTPC überträgt Ihr Cisco Access Point Ihren Cisco CCX-kompatiblen Clients Informationen über den zu verwendenden Leistungsgrad..

Ja, sie ähnelt den beiden anderen Protokollen, die oben erläutert wurden.. DTPC ist jedoch dynamisch, wenn sich der Client näher oder weiter vom AP entfernt. Wenn es sich bei Ihrem Client um CCX handelt, können Sie tatsächlich mehr tun: diesen beeinflussen. Sehr oft hat der AP eine gute 9 dBi Patch-Antenne und der Client hat eine schlechte Gummiente 2,2 dBi Antenne. Ihr Client hört den AP gut, aber das Client-Signal geht im umgebenden Geräusch verloren und Ihr AP hört es nicht gut (trotz Antennengewinn auch verbessert das empfangene Signal). Ihr Client sollte seinen Leistungsgrad erhöhen, aber er weiß nicht, dass der Access Point ihn nicht gut hört.. Sie weiß nur, dass der Access Point (der Client) gut hört und von diesem empfangenen Signal seinen eigenen Leistungsstand abzieht. Wenn Ihr Client CCX ist, kann der Access Point dem Client sagen: "Ich höre Sie nicht gut, erhöhen Sie Ihre Leistung auf 20 mW", oder "Sie brauchen nicht zu schreien! Reduzieren Sie den Stromverbrauch auf 5 mW, was Ihren Akku spart." In diesen Informationen kann der Access Point Maximen kommunizieren ("Erhöhen Sie Ihre Leistung wieder, aber nicht über 50 mW hinaus").