Identifizieren der Radarerkennung in DFS-Kanälen (Dynamic Frequency Selection)

Inhalt

Einleitung

In diesem Dokument wird die Radarerkennung in der DFS-Kanaltheorie (Dynamic Frequency Selection) beschrieben und es wird erläutert, wie die Auswirkungen auf Wireless-Netzwerke gemindert werden können.

Hintergrundinformationen

In den meisten Zulassungsdomänen müssen 802.11-Stationen Dynamic Frequency Selection (DFS) verwenden, wenn sie mit einigen oder allen Kanälen im 5-GHz-Band verwendet werden. (Schauen Sie in den jeweiligen Tabellen für Kanäle und maximale Leistung nach, welche Kanäle DFS für einen bestimmten Access Point/eine bestimmte Domäne erfordern.)

802.11-Stationen müssen, bevor sie in einem DFS-Kanal senden, überprüfen (60 Sekunden lang warten), dass keine Radaraktivität vorhanden ist. Wenn eine 802.11-Funkeinheit Radar erkennt, während der DFS-Kanal verwendet wird, muss dieser Kanal schnell entfernt werden. Wenn also ein Funkgerät Radar in seinem Dienstkanal erkennt und dann auf einen anderen DFS-Kanal umschaltet, führt dies (mindestens) zu einem Ausfall von einer Minute.

Wenn ein Access Point (AP) einen DFS-Kanal verwendet und ein Radarsignal erkannt wird, führt der AP folgende Schritte aus:

- Stoppt die Übertragung von Datenframes auf diesem Kanal
- Sendet eine 802.11h Channel-Switch-Ankündigung.
- Trennt Clients
- Wählt einen anderen Kanal aus der Liste der dynamischen Kanalzuweisung aus
    - Wenn der ausgewählte Kanal kein DFS ist, aktiviert AP Beacons und akzeptiert Client-Zuordnungen.
    - Wählt der WAP einen erforderlichen DFS-Kanal, wird der neue Kanal 60 Sekunden lang auf Radarsignale gescannt. Wenn der neue Kanal keine Radarsignale enthält, aktiviert der WAP Beacons und akzeptiert Client-Zuordnungen. Wird ein Radarsignal erkannt, wählt der AP einen anderen Kanal

DFS-ausgelöste Kanaländerungen wirken sich auf die Client-Konnektivität aus. Wenn wir die AP-Protokolle überprüfen, werden Meldungen wie die folgenden angezeigt:

Für COS-APs

```
[*04/27/2017 17:45:59.1747] Radar detected: cf=5496 bw=4 evt='DFS Radar Detection Chan = 100'
[*04/27/2017 17:45:59.1749] wcp/dfs :: RadarDetection: radar detected
[*04/27/2017 17:45:59.1749] wcp/dfs :: RadarDetection: sending packet out to capwapd, slotId=1, msgLen=3
```

Für IOS-APs

```
Feb 10 17:15:55: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5320 MHz
Feb 10 17:15:55: %DOT11-6-FREQ_USED: Interface Dot11Radio1, frequency 5520 selected
Feb 10 17:15:55: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface Dot11Radio1 due to channel ch
```

Fehlerhafte Ereignisse mit DFS-Kanälen

Ein "falsches DFS-Ereignis" liegt vor, wenn ein Funkmodul Radar falsch erkennt. Es erkennt ein Energiemuster, von dem es annimmt, dass es Radar ist, obwohl es es nicht ist (es ist möglicherweise ein Signal von einem nahe gelegenen Client-Funkgerät). Es ist sehr schwierig festzustellen, ob Radarerkennungsereignisse "falsch" sind. Wenn sich mehrere AP-Funkeinheiten auf demselben DFS-Kanal an demselben Ort befinden, kann man davon ausgehen, dass, wenn **ein einziger** AP Radar zu einem bestimmten Zeitpunkt erkennt, dies wahrscheinlich eine Falscherkennung ist, während mehrere Funkeinheiten Radar zur gleichen Zeit erkennen, es wahrscheinlich ein "echtes" Radar ist.

Cisco hat die Fähigkeit seiner Access Points, zwischen echten und falschen Radarsignalen zu unterscheiden, in vielerlei Hinsicht verbessert. Es ist jedoch nicht möglich, alle falschen Radarsignale vollständig zu eliminieren.

Wenn DFS-Kanäle mit dichten Client-Populationen verwendet werden, muss man sich generell darauf vorbereiten, bis zu vier falsche DFS-Ereignisse pro AP-Funk zu behandeln, ebenso wie natürlich echte Radarereignisse.

Um die Auswirkungen dieser Ereignisse zu mindern/zu reduzieren, können wir:

- **20-MHz-Kanalbreite** zur besseren Wiederverwendung von Nicht-DFS-Kanälen

- **Vermeiden von DFS-Kanälen**
  - Für die FCC-Domäne: Es gibt 9 Nicht-DFS-Kanäle (36-48,149-165). Mit Ausnahme von Bereitstellungen mit sehr hoher Dichte sind dies ausreichend Kanäle (wenn 20 MHz breit verwendet wird), um bei voller (14-17 dBm) Leistung eine vollständige Abdeckung mit tolerierbaren Co-Channel-Interferenzen bereitzustellen
  - Für die ETSI-Domäne: Es gibt nur vier Nicht-DFS-Kanäle (36-48 UNII-1).
    - Kanalzuweisungen so berücksichtigen, dass im Abdeckungsbereich mindestens ein UNII-1-Kanal verfügbar ist
    - Verwenden Sie dann DFS-Kanäle, um zusätzliche Kapazität bereitzustellen.
- **Zur Reduzierung der Auswirkungen von DFS-Ereignissen**
  - 802.11h Channel Announcement aktivieren - standardmäßig auf WLC aktiviert
  - Smart DFS deaktivieren - standardmäßig auf WLC aktiviert
- **Verwendung von CleanAir-APs mit überlegenen Radarerkennungsfunktionen**
  - Die APs der Serien 1700, 2700, 3700, 1570, 2800, 3800, 4800 und 1560 können CleanAir-Hardware zur Unterstützung zusätzlicher DFS-Signalfilterung verwenden, um falsche Ereignisse zu vermeiden.
    - Für 1700, 2700, 3700, 1570, 2800, 3800: verfügbar in den Versionen 8.2.170.0, 8.3.140.0, 8.5.110.0 und 8.6 (Cisco Bug-ID) CSCve35938, Cisco Bug-ID CSCvf38154,

Cisco Bug-ID CSCvg43083)
    - Für 1560: verfügbar in den Versionen 8.5MR4 und 8.8MR1 (Cisco Bug-ID CSCve31869)
- **Wenn DFS-Kanäle auf Nicht-CleanAir-APs benötigt werden**
    - Ein Abstand von 20 MHz zwischen den Kanälen bietet Vorteile für APs, die nicht CleanAir sind (z. B. 18XX, 1540). Beispiel: use 52, (skip 56), use 60, (skip 64), use 100, (skip 104), use 108, ...
    - Access Points der Serie 1800 verfügen über eine verbesserte Radarerkennung in den Versionen 8.3.140.0, 8.5.120.0 und 8.6 Cisco Bug ID (CSCvg62039, Cisco Bug ID CSCvf21657.)

Referenzen

Dynamische Frequenzauswahl

Dynamische Frequenzauswahl - DFS-Aktionen verstehen

Weitere Informationen

Frequenzfreigabe im 5-GHz-Band - DFS Best Practices (IEEE)

Grundlegende Radaruntersuchung für drahtlose Mesh-Netzwerke

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.