Panoramica su 802.11h, controllo della potenza di trasmissione (TPC) e selezione dinamica della frequenza

Sommario

Introduzione

Questo documento offre una panoramica su una sottoparte dello standard wireless 802.11: 802.11h e l'impatto di questo emendamento sulle installazioni wireless e a cosa si traduce in termini di configurazione. L'emendamento è inteso a introdurre due caratteristiche principali: Dynamic Frequency Selection (DFS) e Transmit Power Control (TPC). DFS, in quanto gestione dello spettro (principalmente per cooperare con i radar) e TPC, per limitare l'"inquinamento" complessivo da RF dei dispositivi wireless.

Prerequisiti

Requisiti

Questo documento richiede solo una conoscenza di base del protocollo Wi-Fi o 802.11. Tuttavia, si concentra su problemi specifici delle installazioni all'aperto e sarà meglio compreso con una piccola esperienza di installazione Wi-Fi.

Componenti usati

Un Cisco Wireless Lan Controller (WLC) sul software 8.0 viene utilizzato solo per riferimento alla configurazione.

DFS

Il DFS è incentrato sul rilevamento e l'eliminazione dei radar. Radar è l'acronimo di "Radio Detection and Range". In passato, i radar operavano in gamme di frequenza dove erano l'unico

tipo di dispositivo che operava lì. Ora che le agenzie di regolazione stanno aprendo queste frequenze ad altri usi (come le reti LAN wireless), è necessario che questi dispositivi funzionino secondo i radar.

Il comportamento generale di un dispositivo conforme al protocollo DFS è quello di poter rilevare quando un radar occupa il canale, quindi smettere di utilizzare quel canale occupato, monitorare un altro canale e saltare su di esso se è chiaro. (cioè, anche lì nessun radar).

Il processo di rilevamento di un radar da parte di una radio è un'operazione complessa che in realtà non fa parte dello standard. Quindi, possono verificarsi rilevamenti radar sbagliati ed è un'arte che combina l'algoritmo del fornitore Wi-Fi con le funzionalità del chip Wi-Fi. Tuttavia, il rilevamento stesso è obbligatorio per l'agenzia di regolamentazione e definito in modo chiaro. Di conseguenza, i parametri di scansione non sono configurabili.

DFS è stato richiesto sin dall'inizio per i dispositivi ETSI (European Telecommunication Standard Institute) che operano nell'Unione europea (e nei paesi che seguono le norme ETSI) nella banda ETSI 5 ghz. Non è necessariamente obbligatorio in altre parti del mondo e dipende anche dalla gamma di frequenza. L'American Federal Communication Commission (FCC) ha ora reso obbligatorio l'uso di una gamma di frequenze estesa UNII-2 e UNII-2 come l'ETSI.

Le operazioni DFS utilizzano metodi diversi per lo scambio di informazioni tra le stazioni. Le informazioni possono essere inserite in elementi specifici nella risposta del beacon o della sonda, ma un frame specifico può essere utilizzato anche per riportare le informazioni: frame azione. Lo introdurremo dopo che avremo spiegato quando entreranno in gioco.

Ulteriori informazioni sui radar

I radar possono essere fissi (spesso aeroporti civili o basi militari, ma anche radar meteorologici) o mobili (navi). Una stazione radar trasmetterà periodicamente una serie di impulsi potenti e osserverà i riflessi. Poiché l'energia riflessa nel radar è molto più debole del segnale originale, il radar deve trasmettere un segnale molto potente. Inoltre, poiché l'energia riflessa nel radar è molto debole, potrebbe confonderla con altri segnali radio (come ad esempio una LAN wireless).

Poiché la banda a 2,4 GHz non è radar, le regole DFS si applicano solo alla banda a 5,250 -5,725 GHz.

Quando la radio rileva un radar, deve smettere di utilizzare il canale per almeno 30 minuti per proteggere il servizio. Controlla quindi un altro canale e può iniziare a utilizzarlo dopo almeno 1 minuto se non è stato rilevato alcun radar.

Gli argomenti seguenti sono più correlati alla risoluzione dei problemi in un ambiente Cisco che a una spiegazione sullo standard. Tuttavia, alcuni punti potrebbero interessare tutti e sono abbastanza brevi da essere brevemente spiegati qui di seguito.

DFS in Cisco WLC

DFS è spesso collegato a Mesh ma è semplicemente correlato all'esterno (o anche alle aree interne che ascoltano segnali esterni e operano su canali interni/esterni). Quando un access point sente un radar, cambia canale e blocca il canale precedente per 30 minuti. Questo è piuttosto maleducato con i clienti. "Annuncio di canale" è una bella funzione in cui l'AP dice al cliente che sta escludendo questo canale e verso quale canale si sta spostando.

A meno che non si utilizzi un backhaul doppio, tutti i punti di accesso a rete radice (RAP) e i punti di accesso figlio a rete (MAP) funzionano sullo stesso canale. Così può accadere che solo una MAP rilevi il radar. Sarà quindi l'unico a cambiare canale e non sarà disponibile a parlare con gli altri punti di accesso per almeno 30 minuti (il tempo di tornare su questo canale). Se si desidera che l'intero backhaul si sposti non appena un punto di accesso rileva un radar, è possibile attivare la funzione di "annuncio del canale" e il punto di accesso che rileva il radar comunica agli altri (incluso il punto di accesso) prima di cambiare canale in modo che si spostino tutti insieme. Tutti eseguiranno quindi la scansione di un altro canale per 1 minuto, definito periodo di silenzio. In questo modo si evita che il nuovo canale contenga anche un radar.

Questo menu è disponibile in Wireless->802.11a->DFS nell'interfaccia Web del WLC

Impatto delle regole DFS

Quando si passa a un nuovo canale DFS, un punto di accesso deve ascoltare in silenzio il supporto per un minuto prima di poter trasmettere qualsiasi cosa (come un beacon) per essere certi che nessun radar stia operando su quel canale. I clienti non hanno tale responsabilità e sono autorizzati a inviare frame wifi se un punto di accesso è già presente e beaconing sul canale, questo lascia tutta la responsabilità

y sulle spalle dell'AP. Alcuni canali, tra cui 120, 124 e 128, prevedono regole specifiche in base alle quali un access point deve attendere 10 minuti prima di poter utilizzare i canali.

Ciò significa che i client, quando si spostano su un canale DFS, devono in genere attendere oltre 100 ms per poter ascoltare un beacon. Ciò significa che la scansione è molto costosa in quanto il client non è autorizzato a inviare richieste di probe su un nuovo canale e deve attendere un beacon. Molti fornitori di dispositivi wifi client lo sanno e non assegnano priorità ai canali DFS nell'algoritmo di roaming/scansione. I client non eseguono molto spesso la scansione dei canali DFS a causa dei costi.

Rilevamento radar errato

C'è un delicato equilibrio tra essere abbastanza sensibili per soddisfare i requisiti DFS (rilevamento radar) e non essere troppo sensibili per evitare false rilevazioni. La causa più comune di un rilevamento errato è, per ragioni di costo, l'inserimento di un altro punto di accesso nello stesso punto (ad esempio sullo stesso polo). Anche se l'access point utilizza un altro canale, se il canale è vicino, alcuni impulsi possono verificarsi fuori banda per l'altro access point, ma vengono visti come impulsi in banda e erroneamente presi come radar. La soluzione migliore è un'attenta pianificazione dei canali e il posizionamento dei punti di accesso.

Un'altra causa è un radar che ha una trasmissione del segnale sporca off-channel o è così potente sul suo canale che ha una trasmissione a banda laterale sui canali adiacenti. Quindi, anche se l'access point è sul canale accanto al radar, il radar sta inviando alcuni segnali laterali sul canale dell'access point facendo credere all'access point che un radar stia operando sul canale, anche se non lo è. La soluzione qui è ancora quella di modificare il canale e il posizionamento AP.

Recentemente è stato anche osservato che alcuni dispositivi (o client) di terze parti legittimi avevano il proprio chipset Wi-Fi che a volte inviava impulsi simili a segnali radar. È una regolazione continua per garantire che l'algoritmo DFS rilevi solo radar reali. Potrebbe essere utile controllare le note sulla versione per individuare gli ID dei bug in relazione ai miglioramenti dell'algoritmo DFS.

Gli access point Cisco con chip Cleanair o Rf ASIC possono sfruttare questo analizzatore di spettro per rilevare i radar con una maggiore precisione. Generalmente hanno un numero molto minore di falsi allarmi positivi, in quanto sia il chip wifi che il chip ASIC Cleanair/RF analizzano i segnali e un evento radar si verifica solo se entrambi concordano che il segnale udito proviene da un radar. Ciò consente un livello di accuratezza tale che i punti di accesso radio solo Wi-Fi non possono avvicinarsi in remoto.

Debug

Gli eventi DFS vengono individuati principalmente con i traplog, ma le alternative sono:

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

AP li ricorderà fino al prossimo riavvio.

I clienti che utilizzano punti di accesso esterni nell'UE o in regioni con normative simili dovrebbero consentire questa opzione.
>abilitazione config advanced 802.11a channel outdoor-ap-dca

Se attivato, il controller non eseguirà il controllo dei canali non DFS nell'elenco DCA. Lo stato predefinito è Off (comportamento esistente).

Ulteriori informazioni su CSCsl90630.

Modalità TPC vs DTPC vs World

Avete mai sentito parlare di TPC (controllo della potenza di trasmissione), DTPC (controllo dinamico della potenza di trasmissione) e della modalità World? Sembrano uguali, ma in realtà non fanno le stesse cose... diamo un'occhiata veloce a ciascuno di loro:

- **World Mode** è probabilmente il più vecchio. È la modifica 802.11d del protocollo Wi-Fi. Si tratta di una funzionalità che è possibile configurare sui punti di accesso autonomi (aIOS) e che è attivata per impostazione predefinita sui punti di accesso lightweight e tramite la quale un client in modalità Mondo riceve i parametri radio dal punto di accesso. I parametri sono in realtà canali e

livelli di alimentazione. Ma non sbagliare. "Channels" ha una "s". Non è il canale su cui il client deve trovarsi! Per ascoltare il punto di accesso, il client deve comunque trovarsi sul canale giusto. Quindi quello che la Modalità Mondiale riguarda è "la lista dei canali consentiti in questo paese" e "i livelli di potenza consentiti in questo paese".

-**TPC, Transmit Power Control**, è in realtà una funzione di 802.11h insieme a DFS con cui il punto di accesso può definire regole locali per la massima potenza di trasmissione. Ci sono molte ragioni per cui questo sarebbe utilizzato. È possibile che l'amministratore desideri impostare un altro set di regole oltre al massimo del dominio normativo a causa di regole locali o ambienti più specifici. Un'altra potrebbe essere che l'amministratore sa che si tratta di un'installazione Wi-Fi molto densa con una copertura intensa : Pertanto, gli access point si impostano su una potenza di trasmissione inferiore (grazie all'algoritmo RRM) e il TPC è un modo statico per forzare i client a ridurre anche la loro potenza e quindi la loro copertura in modo da non disturbare i client/access point vicini che si trovano sullo stesso canale.

-**DTPC, Dynamic Transmit Power Control**, è simile a TPC ma non ha una relazione diretta. È un sistema proprietario di Cisco. Con DTPC, il punto di accesso Cisco trasmette ai client Cisco CCX informazioni sul livello di alimentazione da utilizzare...

Sì, è vicino agli altri due protocolli spiegati sopra... Tuttavia, il DTPC sarà dinamico man mano che il client si avvicina o si allontana dall'access point. Se il client è CCX, è possibile ottenere maggiori risultati: influenzarla. Molto spesso, l'AP ha una buona 9 dBi antenna patch e il client ha una scarsa antenna di anatra di gomma 2.2 dBi. Il client sente bene l'access point, ma il segnale client si perde nel rumore circostante e l'access point non lo sente bene (nonostante il guadagno dell'antenna migliori anche il segnale ricevuto). Il client deve aumentare il livello di alimentazione, ma non sa che l'access point non lo sente bene... tutto ciò che sa è che (il client) sente bene l'access point e da questo segnale ricevuto deduce il proprio livello di alimentazione. Se il client è CCX, l'access point può dire al client "Non ti sento bene, aumenta la potenza a 20 mW", o "non c'è bisogno di urlare! riduci la corrente a 5 mW, risparmiando la batteria". In queste informazioni, l'access point può comunicare i massimi livelli ("aumentare di nuovo la potenza, ma non superare i 50 mW").