Descripción general de 802.11h, control de potencia de transmisión (TPC) y selección dinámica de frecuencia

Contenido

Introducción

Este documento es una descripción general de una subparte del estándar 802.11 inalámbrico : 802.11h y el impacto de esta enmienda en las implementaciones inalámbricas y a lo que se traduce en términos de configuración. Esta enmienda tenía por objeto presentar dos características principales: Selección dinámica de frecuencia (DFS) y control de potencia de transmisión (TPC). DFS, como gestión del espectro (principalmente para cooperar con radares) y TPC, para limitar la "contaminación" general de RF de los dispositivos inalámbricos.

Prerequisites

Requirements

Este documento sólo requiere una comprensión muy básica del protocolo Wi-Fi o 802.11. Sin embargo, se centra en problemas específicos de las implementaciones en exteriores y se comprenderá mejor con una pequeña experiencia de implementación de Wi-Fi.

Componentes Utilizados

Un controlador de LAN inalámbrica (WLC) de Cisco en el software 8.0 se utiliza solamente para referencia de configuración.

DFS

DFS trata sobre la detección y prevención de radar. Radar significa "detección y medición de radio". En el pasado, los radares solían operar en intervalos de frecuencias donde eran el único

tipo de dispositivo que operaba allí. Ahora que las agencias reguladoras están abriendo esas frecuencias para otros usos (como LAN inalámbrica), es necesario que estos dispositivos funcionen de acuerdo con los radares.

El comportamiento general de un dispositivo que cumple con el protocolo DFS es poder detectar cuándo un radar está ocupando el canal, para luego dejar de usar ese canal ocupado, monitorear otro canal y saltar sobre él si está claro. (es decir, no hay radar también allí).

El proceso para que una radio detecte un radar es una tarea complicada que en realidad no forma parte del estándar. Por lo tanto, pueden producirse detecciones de radar erróneas y se trata de una arte que combina el algoritmo del proveedor de Wi-Fi con las funciones de chip Wi-Fi. Sin embargo, la propia detección es obligatoria por el organismo regulador y está claramente definida. Por lo tanto, los parámetros de escaneo no se pueden configurar.

El DFS se ha exigido desde el principio para los dispositivos del Instituto Europeo de Normas de Telecomunicaciones (ETSI) que trabajan en la Unión Europea (y en los países que siguen las normas ETSI) en la banda ETSI 5ghz. No es necesariamente obligatorio en otras partes del mundo y también depende del intervalo de frecuencia. La Comisión Federal de Comunicaciones de Estados Unidos (FCC, por sus siglas en inglés) ahora lo ha hecho obligatorio para UNII-2 y UNII-2 para un rango de frecuencia ampliado como ETSI.

Las operaciones de DFS utilizan diferentes maneras de intercambiar información entre estaciones. La información se puede incluir en elementos específicos de la respuesta de baliza o sonda, pero también se puede utilizar un marco específico para informar información: el marco de acción. Lo presentaremos después de explicarlo cuando entren en juego.

Más información sobre los radares

Los radares pueden ser fijos (a menudo, aeropuertos civiles o bases militares, pero también radar meteorológico) o móviles (buques). Una estación de radar transmitirá periódicamente un conjunto de impulsos potentes y observará los reflejos. Como la energía reflejada en el radar es mucho más débil que la señal original, el radar tiene que transmitir una señal muy potente. Además, como la energía reflejada en el radar es muy débil, podría confundirlo con otras señales de radio (como una LAN inalámbrica para dar un ejemplo).

Debido a que la banda de 2,4 Ghz no tiene radar, las reglas DFS sólo se aplican a la banda de 5,250-5,725 Ghz.

Cuando la radio detecta un radar, debe dejar de usar el canal durante al menos 30 minutos para proteger ese servicio. Luego monitorea otro canal y puede comenzar a usarlo al menos después de 1 minuto si no se detecta ningún radar.

El siguiente tema está más relacionado con la resolución de problemas en un entorno de Cisco que con la explicación del estándar. Sin embargo, algunos puntos pueden ser de interés para todos y son lo suficientemente cortos como para explicarlos brevemente a continuación.

DFS en Cisco WLC

El DFS suele estar vinculado a la malla, pero se relaciona simplemente con el exterior (o incluso con zonas interiores que oyen señales exteriores y que funcionan con canales interiores o exteriores). Cuando un AP escucha un radar, cambiará de canal y prohibirá el canal anterior durante 30 minutos. Esto es bastante grosero con los clientes. "Anuncio de canal" es una

característica agradable donde el AP le dice al cliente que está excluyendo este canal y hacia qué canal se está moviendo ahora.

A menos que utilice una red de retorno dual, todos los AP de malla raíz (RAP) y los AP de malla secundaria (MAP) funcionan en el mismo canal. Por lo tanto, puede ocurrir que solamente un MAP detecte el radar. Luego será el único en cambiar el canal y no estará disponible para hablar con los otros AP durante al menos 30 minutos (el tiempo para volver en este canal). Si desea que toda la red de retorno se mueva tan pronto como un AP detecte un radar, entonces puede habilitar la función de "anuncio de canal" y el AP que detecte el radar se lo dirá a los otros (incluyendo el RAP) antes de cambiar de canal para que todos se muevan juntos. A continuación, todos escanearán otro canal durante 1 minuto, lo que se conoce como el período de inactividad. Esto es para asegurarse de que el nuevo canal no contenga un radar también.

Este menú está disponible en Wireless->802.11a->DFS en la interfaz web del WLC

impacto de las reglas DFS

Un AP, cuando se mueve a un nuevo canal DFS, tiene que escuchar silenciosamente al medio durante un minuto antes de que se le permita transmitir cualquier cosa (como una baliza) para asegurarse de que ningún radar esté funcionando actualmente en ese canal. Los clientes no tienen tal responsabilidad y se les permite enviar tramas wifi si un AP ya está presente y permaneciendo en el canal, esto deja toda la responsabilidad

y en los hombros del AP. Ciertos canales como 120, 124 y 128 tienen reglas específicas donde un AP incluso tiene que esperar 10 minutos antes de poder usar esos canales.

Esto significa que los clientes, cuando se mueven a un canal DFS, normalmente tendrán que esperar más de 100 ms para escuchar una baliza. Esto significa que el esfuerzo de escaneo es muy costoso ya que al cliente no se le permite enviar solicitudes de sonda en un nuevo canal y tiene que esperar por una baliza. Muchos proveedores de dispositivos Wi-Fi cliente lo saben y desasignan las prioridades de los canales DFS en su algoritmo de roaming/escaneo. Los clientes no escanean los canales DFS muy a menudo debido al coste de hacerlo.

Detección de radar incorrecta

Existe un delicado equilibrio entre ser lo suficientemente sensible como para cumplir los requisitos de las DAAT (detectar radares) y no ser demasiado sensible para evitar la detección falsa. La causa más común de la detección incorrecta es, por razones de costo, colocar otro AP co-ubicado (en el mismo poste por ejemplo). Incluso si ese AP está usando otro canal, si ese canal está cerca, algún pulso puede ocurrir fuera de banda para este otro AP pero se verá como

pulsos dentro de banda y se tomará incorrectamente como un radar. La mejor solución es una cuidadosa planificación de canales y colocación de puntos de acceso.

Otra causa es un radar que tiene alguna transmisión de señal fuera de canal sucia o es tan potente en su canal que tiene transmisión de banda lateral en canales adyacentes. Así que incluso si el AP está en el canal junto al radar, el radar está enviando algunas señales laterales en el canal AP haciendo que el AP crea que un radar está funcionando en el canal, aunque no lo está. La solución aquí todavía está por cambiar la ubicación del canal AP y AP.

También se ha visto recientemente que algunos dispositivos (o clientes) legítimos de terceros tenían su chipset Wi-Fi que a veces enviaba impulsos parecidos a señales de radar. Se trata de un ajuste fino constante para asegurarse de que el algoritmo DFS sólo detecta radares reales. Puede que valga la pena verificar las notas de la versión para las ID de bug con respecto a las mejoras del algoritmo DFS.

Los AP de Cisco que tienen un chip Cleanair o Rf ASIC pueden aprovechar este analizador de espectro para detectar radares con mucha más precisión. Por lo general, tendrán menos alertas positivas falsas ya que tanto el chip wifi como el chip Cleanair/RF ASIC analizarán las señales y un evento de radar sólo ocurrirá si ambos coinciden en que la señal escuchada vino de un radar. Esto permite un nivel de precisión que los AP de radio solamente con Wifi no pueden aproximarse remotamente.

Depuraciones

Principalmente detecta eventos DFS con tramas, pero las alternativas son:

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

AP recordará esos hasta el siguiente reinicio.

Los clientes que implementen AP exteriores en la UE o regiones con regulaciones similares deberían habilitar esta opción.
>config advanced 802.11a channel outside-ap-dca enable

Cuando está activado, Controller no realizará la verificación de los canales no DFS en la lista DCA. El estado predeterminado es Off (Desactivado) (comportamiento existente).

Más detalles sobre CSCsl90630.

TPC frente a DTPC frente al modo mundial

¿Ha oído hablar de TPC (control de potencia de transmisión), DTPC (control de potencia de transmisión dinámica) y del modo mundial? Se ven iguales, pero en realidad no hacen lo mismo... echemos un vistazo rápido a cada uno de ellos:

- **World Mode** es probablemente el más antiguo. Se trata de la enmienda 802.11d del protocolo Wi-Fi. Se trata de una función que puede configurar en los puntos de acceso autónomos (aIOS) y

que está activada de forma predeterminada en los AP ligeros, y por la cual un cliente en el modo mundial recibe sus parámetros de radio del punto de acceso.Los parámetros son en realidad canales y niveles de alimentación. Pero no se equivoquen. "Canales" tiene una "s". No es el canal en el que debería estar el cliente. Para escuchar el punto de acceso, el cliente debe estar en el canal correcto. De lo que se trata World Mode es de "la lista de canales permitidos en este país" y "los rangos de nivel de energía permitidos en este país".

- **TPC, Control de potencia de transmisión**, es en realidad una función de 802.11h junto con DFS mediante la cual el punto de acceso puede definir reglas locales para la máxima potencia de transmisión. Hay muchas razones por las que esto se usaría. Una podría ser que el administrador desea establecer otro conjunto de reglas que no sea el máximo del dominio regulador debido a reglas locales o entorno más específicos. Otra cosa podría ser que el administrador sabe que es una implementación Wi-Fi muy densa con una cobertura intensa : Por lo tanto, los AP se establecen en una potencia de transmisión inferior (gracias al algoritmo RRM) y el TPC es una manera estática de obligar a los clientes a reducir también su potencia y, por lo tanto, reducir su cobertura para que no perturben a los clientes/AP vecinos que están en el mismo canal.

-**DTPC, que es Control de Potencia de transmisión dinámica**, se parece al TPC pero no tiene relación directa. Es un sistema propiedad de Cisco. Con DTPC, el punto de acceso de Cisco transmite a sus clientes que cumplen con Cisco CCX información sobre el nivel de alimentación que debe utilizar...

Sí, está cerca de los otros dos protocolos explicados anteriormente... Sin embargo, el DTPC será dinámico a medida que el cliente se acerque o se aleje del AP. Si su cliente es CCX, puede hacer más: influir en él. Muy a menudo, el AP tiene una buena antena de parche de 9 dBi y el cliente tiene una pobre antena de conducto de goma de 2.2 dBi. Su cliente oye bien el AP, pero la señal del cliente se pierde en el ruido circundante y su AP no la oye bien (a pesar de la ganancia de la antena también mejora la señal recibida). Su cliente debe aumentar su nivel de potencia, pero no sabe que el AP no lo oye bien... todo lo que sabe es que él (el cliente) oye bien el AP, y de esta señal recibida se deduce su propio nivel de potencia. Si su cliente es CCX, el AP puede decirle al cliente "No le oigo bien, aumente su potencia a 20 mW", o "¡no necesitan gritar! reduzca la potencia a 5 mW, lo que ahorrará la batería". En esta información, el AP puede comunicar los máximos ("aumentar su potencia de nuevo, pero no exceder los 50 mW").