Identificación de la detección de radares en canales de selección dinámica de frecuencia (DFS)

Contenido

Introducción

Este documento describe la detección de radares en la teoría de canales de selección dinámica de frecuencia (DFS) y cómo mitigar su impacto en las redes inalámbricas.

Antecedentes

En la mayoría de los dominios normativos, las estaciones 802.11 deben utilizar la selección dinámica de frecuencia (DFS) cuando se utilizan con algunos o todos los canales de la banda de 5 GHz. (Consulte las hojas de cálculo Canales y Potencia máxima correspondientes para ver los canales específicos que requieren DFS para un punto de acceso o dominio determinado.)

Las estaciones 802.11, antes de transmitir en un canal DFS, deben validar (escuchar durante 60 segundos) que no hay actividad de radar en ellas. Además, si una radio 802.11 detecta un radar mientras se utiliza el canal DFS, debe abandonar ese canal rápidamente. Por lo tanto, si una radio detecta un radar en su canal de servicio, luego cambia a otro canal DFS, esto impone (al menos) una interrupción de un minuto.

Cuando un punto de acceso (AP) utiliza un canal DFS y se detecta una señal de radar, el AP entonces:

- Detiene la transmisión de tramas de datos en ese canal
- Difunde un anuncio de switch de canal 802.11h.
- Desasocia clientes
- Selecciona un canal diferente de la lista DCA (asignación de canal dinámico)
    - Si el canal seleccionado no es DFS, AP habilita las balizas y acepta las asociaciones de clientes
    - Si el AP selecciona un canal requerido por DFS, explora el nuevo canal en busca de señales de radar durante 60 segundos. Si no hay señales de radar en el nuevo canal, el AP habilita las balizas y acepta las asociaciones del cliente. Si se detecta una señal de radar, el punto de acceso selecciona un canal diferente

Los cambios de canal desencadenados por DFS afectan a la conectividad del cliente. Cuando examinamos los registros de AP, podemos ver mensajes similares a los siguientes:

Para los AP COS

```
[*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
```

Para AP IOS

```
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
```

Eventos falsos con canales DFS

Un "evento DFS falso" es cuando una radio detecta un radar falsamente. Ve un patrón de energía que cree que es el radar, aunque no lo es (posiblemente es una señal de una radio cliente cercana). Es muy difícil determinar si los eventos de detección por radar son "falsos". Si hay múltiples radios AP en el mismo canal DFS en la misma ubicación, entonces podemos asumir, como regla general, que si **un solo** AP detecta el radar en un momento dado, entonces es probablemente una falsa detección, mientras que si múltiples radios detectan el radar al mismo tiempo, es probable que sea un radar "real".

Cisco ha realizado numerosas mejoras en la capacidad de nuestros puntos de acceso para distinguir entre señales de radar reales y falsas; sin embargo, no es posible eliminar por completo la detección de radares falsos.

En general, si los canales DFS se utilizan con poblaciones de clientes densas, uno debe prepararse para manejar hasta cuatro eventos DFS falsos por radio AP, así como, por supuesto, eventos de radar reales.

Con el fin de mitigar/reducir el impacto de estos eventos, podemos:

- **Utilice un ancho de canal de 20 MHz**, que también permite una mejor reutilización de los canales no DFS

- **Evitar canales DFS**
  - Para el dominio FCC: hay 9 canales no DFS (36-48.149-165). Excepto en el caso de implementaciones muy densas, se trata de canales suficientes (si se utiliza una banda de 20 MHz de ancho) para proporcionar una cobertura completa con interferencias de canal compartido tolerables a una potencia máxima (14-17 dBm)
  - Para el dominio ETSI: solo hay cuatro canales no DFS (36-48 UNII-1)
    - Considere las asignaciones de canal de modo que haya al menos un canal UNII-1 disponible en todo el área de cobertura
    - A continuación, utilice los canales DFS para proporcionar capacidad adicional.
- **Para reducir el impacto de los eventos de DFS**
  - Activar anuncio de canal 802.11h: habilitado de forma predeterminada en el WLC
  - Desactivar Smart DFS: habilitado de forma predeterminada en WLC
- **Utilice puntos de acceso CleanAir con excelentes funciones de detección de radares**
  - Los AP de las series 1700, 2700, 3700, 1570, 2800, 3800, 4800 y 1560 pueden utilizar el hardware CleanAir para soportar el filtrado de señales DFS adicional para evitar eventos falsos.
    - Para 1700, 2700, 3700, 1570, 2800, 3800: está disponible en 8.2.170.0, 8.3.140.0, 8.5.110.0 y 8.6. (Id. de error de Cisco CSCve35938, Id. de error de Cisco CSCvf3815444 Id. de error de Cisco CSCvg43083)
    - Para 1560: está disponible en las versiones 8.5MR4 y 8.8MR1 (Id. de error de Cisco CSCve31869)
- **Si se necesitan canales DFS en puntos de acceso que no sean CleanAir**
  - Un espacio de 20 MHz entre canales beneficia a puntos de acceso que no son CleanAir (como 18XX, 1540). Ejemplo: use 52, (skip 56), use 60, (skip 64), use 100, (skip 104), use 108, ...
  - Los AP de la serie 1800 han mejorado la detección de radares en 8.3.140.0, 8.5.120.0 y 8.6 Id.

de bug de Cisco (CSCvg62039, Id. de bug de Cisco CSCvf21657.)

Referencias

Selección dinámica de frecuencia

Comprender la selección de frecuencia dinámica: acciones de DFS

Más información

Uso compartido del espectro en la banda de 5 GHz: mejores prácticas de DFS (IEEE)

Sondeo por radar básico para redes de malla inalámbricas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).