Visão geral do 802.11h, Controle de potência de transmissão (TPC) e Seleção de frequência dinâmica

Contents

Introduction

Este documento é uma visão geral sobre uma subparte do padrão 802.11 sem fio : 802.11h e o impacto dessa emenda nas implantações sem fio e o que ela significa em termos de configuração. A presente alteração visa introduzir duas características principais: Seleção dinâmica de frequência (DFS) e Controle de potência de transmissão (TPC). DFS, como gerenciamento de espectro (principalmente para a cooperação com radares) e TPC, para limitar a "poluição" geral de RF de dispositivos sem fio.

Prerequisites

Requirements

Este documento requer apenas uma compreensão muito básica do protocolo Wi-Fi ou 802.11. No entanto, ela se concentra em problemas específicos de implantações externas e será mais bem compreendida com uma pequena experiência de implantação de Wi-Fi.

Componentes Utilizados

Um Cisco Wireless Lan Controller (WLC) no software 8.0 é usado somente para referência de configuração.

DFS

O DFS tem tudo a ver com detecção e prevenção de radar. Radar significa "detecção e alcance de rádio". Antigamente, os radares operavam em faixas de frequência onde eram o único tipo de

dispositivo operando ali. Agora que as agências reguladoras estão abrindo essas frequências para outros usos (como a LAN sem fio), é necessário que esses dispositivos operem de acordo com os radares.

O comportamento geral de um dispositivo em conformidade com o protocolo DFS é poder detectar quando um radar está ocupando o canal, parar de usar esse canal ocupado, monitorar outro canal e pular sobre ele se estiver limpo. (ou seja, nenhum radar lá também).

O processo para um rádio detectar um radar é uma tarefa complicada que na verdade não faz parte do padrão. Assim, detecções erradas de radar podem ocorrer e são uma arte que combina o algoritmo do fornecedor de Wi-Fi com os recursos do chip Wi-fi. No entanto, a detecção propriamente dita é obrigatória pela agência reguladora e claramente definida. Portanto, os parâmetros de verificação não são configuráveis.

O DFS foi necessário desde cedo para os dispositivos ETSI (European Telecommunications Standard Institute, Instituto Europeu de Normas de Telecomunicações) que funcionam na União Europeia (e em países que seguem regulamentos ETSI) na banda ETSI de 5 ghz. Não é necessariamente obrigatório noutras partes do mundo e também depende da gama de frequências. A Comissão Federal de Comunicações Americana (FCC) tornou agora obrigatória para a faixa de frequências estendida UNII-2 e UNII-2, como a ETSI.

As operações de DFS usam diferentes maneiras de trocar informações entre estações. As informações podem ser colocadas em elementos específicos na resposta do beacon ou da sonda, mas um quadro específico também pode ser usado para relatar informações: o quadro de ação. Apresentaremos isso depois de explicarmos quando eles entrarem em jogo.

Mais informações sobre radares

Os radares podem ser fixos (frequentemente aeroportos civis ou bases militares, mas também radares meteorológicos) ou móveis (navios). Uma estação de radar transmitirá periodicamente um conjunto de pulsos potentes e observará as reflexões. Como a energia refletida de volta ao radar é muito mais fraca que o sinal original, o radar tem de transmitir um sinal muito poderoso. Além disso, como a energia refletida de volta ao radar é muito fraca, ela pode confundi-la com outros sinais de rádio (como uma LAN sem fio para dar um exemplo).

Como a banda de 2,4 GHz está livre de radar, as regras do DFS se aplicam somente à banda de 5,250 -5,725 Ghz.

Quando o rádio detecta um radar, deve parar de utilizar o canal durante 30 minutos, pelo menos, para proteger esse serviço. Em seguida, ele monitora outro canal e pode começar a usá-lo após pelo menos 1 minuto se nenhum radar tiver sido detectado.

O tópico a seguir está mais relacionado à solução de problemas em um ambiente da Cisco do que à explicação sobre o padrão. No entanto, alguns pontos podem ser de interesse para todos e são suficientemente curtos para serem explicados brevemente a seguir.

DFS no Cisco WLC

O DFS é frequentemente vinculado à malha, mas está simplesmente relacionado a áreas externas (ou mesmo áreas internas que ouvem sinais externos e operam em canais internos/externos). Quando um AP ouve um radar, ele muda de canal e bane o canal anterior por 30 minutos. Isso é bem grosseiro com os clientes. "Anúncio de canal" é um recurso interessante

em que o AP informa ao cliente que está excluindo esse canal e em direção a qual canal está se movendo agora.

A menos que você esteja usando um backhaul duplo, todos os seus RAPs (Root mesh APs) e MAPs (Mesh child APs) operam no mesmo canal. Assim, pode acontecer que apenas um MAP detecte o radar. Será então o único a mudar de canal e não estará disponível para falar com os outros APs por pelo menos 30 minutos (o tempo de retorno neste canal). Se você quiser que todo o seu backhaul se mova assim que um AP detectar um radar, você poderá ativar o recurso de "anúncio de canal" e o AP que detecta o radar informará os outros (incluindo o RAP) antes de mudar de canal para que todos se movam juntos. Em seguida, todos digitalizarão outro canal por 1 minuto, conhecido como período de silêncio. Isso garante que o novo canal não contenha um radar também.

Este menu está disponível em Wireless->802.11a->DFS na interface da Web da WLC

impacto das regras de DFS

Um AP, ao mover-se para um novo canal DFS, tem de ouvir silenciosamente o meio durante um minuto antes de ser permitido transmitir qualquer coisa (como um beacon) para se certificar de que nenhum radar está atualmente a funcionar nesse canal. Os clientes não têm essa responsabilidade e têm permissão para enviar quadros de wifi se um AP já estiver presente e bebendo no canal, isso deixa toda a responsabilidade

y nos ombros do AP. Certos canais, como 120,124 e 128, têm regras específicas nas quais um AP deve esperar até 10 minutos antes de poder usar esses canais.

Isso significa que os clientes, ao se moverem para um canal DFS, normalmente terão que esperar mais de 100 ms para ouvir um beacon. Isso significa que o esforço de verificação é muito caro, pois o cliente não tem permissão para enviar solicitações de sondagem em um novo canal e tem que esperar por um beacon. Muitos fornecedores de dispositivos wifi clientes sabem disso e despriorizam os canais DFS em seu algoritmo de roaming/varredura. Os clientes não verificam os canais DFS com muita frequência devido ao custo de fazer isso.

Detecção de radar incorreta

Há um equilíbrio delicado entre ser sensível o suficiente para atender aos requisitos do DFS (detectando radares) e não ser muito sensível para evitar uma detecção falsa. A causa mais comum de detecção incorreta é, por razões de custo, colocar outro AP co-localizado (no mesmo polo, por exemplo). Mesmo que esse AP esteja usando outro canal, se esse canal estiver próximo, algum pulso pode ocorrer fora da banda para esse outro AP, mas será visto como

pulsos dentro da banda e tomado incorretamente como um radar. A melhor solução é o planejamento cuidadoso do canal e o posicionamento do AP.

Outra causa é um radar que tem alguma transmissão suja de sinal fora do canal ou é tão potente em seu canal que tem transmissão de banda lateral em canais adjacentes. Assim, mesmo que o AP esteja no canal próximo ao radar, o radar está enviando alguns sinais laterais no canal AP, fazendo com que o AP acredite que um radar está operando no canal, embora não esteja. A solução aqui ainda é alterar o canal de AP e o posicionamento do AP.

Também se viu recentemente que alguns dispositivos (ou clientes) legítimos de terceiros tinham seu chipset Wi-Fi, às vezes enviando pulsos parecidos com sinais de radar. É um ajuste contínuo para garantir que o algoritmo DFS apenas localize radares reais. Talvez valha a pena verificar as notas de versão para IDs de bug com relação às melhorias do algoritmo DFS.

Os APs Cisco que têm um chip ASIC Cleanair ou Rf podem utilizar esse analisador de espectro para detectar radares com muito mais precisão. Normalmente, eles têm muito menos alertas falsos positivos, já que tanto o chip wifi quanto o chip ASIC Cleanair/RF analisarão os sinais e um evento de radar só ocorrerá se ambos concordarem que o sinal ouvido veio de um radar. Isso permite um nível de precisão que os APs de rádio somente Wi-Fi não podem abordar remotamente.

Debugs

Você detecta principalmente eventos de DFS com traplogs, mas as alternativas são:

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

O AP se lembrará delas até a próxima reinicialização.

Os clientes que implementam APs externos na UE ou em regiões com regulamentos semelhantes devem permitir esta opção.
>config advanced 802.11a channel outdoor-ap-dca enable

Quando habilitado, o controlador não realizará a verificação de canais não DFS na lista DCA. O status padrão é Off (Desativado) (comportamento existente).

Mais detalhes sobre o CSCsl90630.

TPC vs DTPC vs World mode

Você já ouviu falar de TPC (Transmit Power Control), DTPC (Dynamic Transmit Power Control) e World Mode? Eles parecem iguais, mas não fazem as mesmas coisas... vamos dar uma olhada rápida em cada um deles:

- **World Mode** é provavelmente o mais antigo. É a alteração 802.11d do protocolo Wi-fi. É um recurso que você pode configurar nos pontos de acesso Autônomos (IOS) e que está ativado por padrão em APs leves e pelo qual um cliente no Modo Mundial recebe seus parâmetros de rádio

do ponto de acesso.Os parâmetros são, na verdade, canais e níveis de energia. Mas não entenda errado. "Channels" tem um "s". Não é o canal no qual o cliente deve estar! Para ouvir o ponto de acesso, o cliente deve estar no canal certo. Então o que o World Mode significa é "a lista de canais permitidos neste país" e "os intervalos de nível de potência permitidos neste país".

-**TPC, Transmit Power Control**, é na verdade um recurso do 802.11h junto com o DFS pelo qual o ponto de acesso pode definir regras locais para máxima potência de transmissão. Há muitas razões pelas quais isso seria usado. Uma delas pode ser que o administrador deseja definir outro conjunto de regras que não o máximo de domínio regulatório devido a regras locais ou ambiente mais específicos. Outra possibilidade é que o administrador saiba que é uma implantação Wi-Fi muito densa com uma cobertura intensa: portanto, os APs se ajustam a uma potência de transmissão mais baixa (graças ao algoritmo RRM) e o TPC é uma forma estática de forçar os clientes a também baixarem sua energia e, portanto, reduzirem sua cobertura para que não perturbem os clientes/APs vizinhos que estão no mesmo canal.

-**DTPC, que é o Controle de potência de transmissão dinâmica**, se aproxima do TPC, mas não tem relação direta. É um sistema proprietário da Cisco. Com o DTPC, seu access point da Cisco transmite aos seus clientes compatíveis com o Cisco CCX informações sobre qual nível de potência usar...

Sim, está perto dos outros dois protocolos explicados acima... No entanto, o DTPC será dinâmico à medida que o cliente se aproxima ou se afasta mais do AP. Se o seu cliente for CCX, você pode realmente fazer mais: influenciá-lo. Frequentemente, o AP tem uma boa antena patch de 9 dBi e o cliente tem uma antena de pato de borracha ruim de 2,2 dBi. Seu cliente ouve bem o AP, mas o sinal do cliente é perdido no ruído ao redor e seu AP não o ouve bem (apesar do ganho da antena também melhorar o sinal recebido). Seu cliente deve aumentar seu nível de energia, mas não sabe que o AP não o ouve bem... tudo o que ele sabe é que (o cliente) ouve bem o AP e, a partir desse sinal recebido, ele deduz seu próprio nível de potência. Se o seu cliente for CCX, o AP poderá dizer ao cliente "Não estou ouvindo bem, aumente sua energia para 20 mW" ou "não precisa gritar! reduza a energia para 5 mW, o que economizará a bateria". Nessas informações, o AP pode comunicar os máximos ("aumente sua energia novamente, mas não ultrapasse 50 mW").