Roaming WGB: Detalhes internos e configuração

Contents

Introduction

A Cisco Workgroup Bridge (WGB) é uma ferramenta muito útil para o projeto e a implantação de uma rede sem fio, pois permite que dispositivos que não usam fio ganhem mobilidade. O WGB fornece muitos detalhes sobre roaming, acesso à segurança, etc., que afetam os cenários de implantação, dependendo das suas necessidades.

Nas versões de código 12.4(25d)JA e posteriores, a Cisco introduziu um conjunto de comandos e alterações para otimizar o uso de WGB em ambientes de roaming de alta velocidade.

Este documento aborda diferentes aspectos de como um WGB funciona, incluindo pontos de decisão de algoritmo de roaming e como configurá-lo para o modelo de uso pretendido.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Solução Cisco Wireless LAN
- Bridge de grupo de trabalho da Cisco

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

O que é uma ponte de grupo de trabalho?

Um WGB é basicamente um ponto de acesso (AP) configurado para atuar como um cliente sem fio em direção a uma infraestrutura e para fornecer conectividade de Camada 2 para os dispositivos conectados à sua interface Ethernet.

Uma implantação WGB típica tem estes componentes:

- Dispositivo WGB, normalmente com pelo menos um rádio e uma interface ethernet
- Uma infraestrutura sem fio, normalmente chamada de AP raiz, que pode ser autônoma ou unificada.
- Um ou mais dispositivos clientes com fio conectados ao WGB. Este documento não cobre cenários de função mista (um rádio como WGB, um rádio como raiz no mesmo AP).

Há três tipos principais de WGB:

- **Cisco WGB**: O Cisco WGB é qualquer AP baseado no Cisco IOS® configurado como WGB (1130, 1240, 1250, etc.). Esse modo usa o protocolo IAPP para informar a infraestrutura de rede dos dispositivos que a WGB aprendeu em sua interface Ethernet. Nesse caso, o Wireless LAN Controller (WLC) ou o AP raiz tem a visibilidade da camada 2 dos dispositivos "suspensos" do WGB.

- **WGB não Cisco:** Este é um dispositivo de terceiros que atua como um WGB, conectando um ou mais dispositivos com fio à infraestrutura sem fio. Eles não suportam o IAPP e permitem apenas um único dispositivo com fio ou fornecem um mecanismo de conversão de endereços MAC, ocultando todos os seus clientes com fio atrás de um único endereço MAC 802.11. Esses tipos de dispositivos precisam de tratamento especial nos quadros ARP (Address Resolution Protocol) e DHCP se a infraestrutura for uma WLC devido às verificações de segurança e ao tratamento de quadros feitos nos controladores.
- **Cisco AP configurado como "Universal WGB"**: Esse é um modo que suprime o mecanismo IAPP, de modo que o WGB possa ser usado para uma infraestrutura Cisco ou APs raiz de terceiros. Nesse caso, o WGB leva o endereço de seu cliente Ethernet, limitando o número de dispositivos atrás dele a um.

A próxima seção enfatiza o cenário de um Cisco WGB usado para infraestruturas autônomas ou WLC.

Cenários de uso

Exemplos de uso típicos de WGB incluem:

- Conectando uma impressora cabeada à rede
- Diferentes implantações de fabricação, nas quais não é viável ou prático passar um cabo até o dispositivo com fio
- Implantações em veículos, em que o WGB fornece conectividade de um carro, trem metro etc. para uma rede wireless externa
- Câmeras com fio

Cada exemplo tem seus próprios requisitos em termos de:

- Largura de banda necessária para suportar o aplicativo que será executado sobre a infraestrutura sem fio
- Tolerância de retardo de roaming - Quanto tempo leva para o WGB se mover do AP atual para o próximo enquanto o dispositivo está se movendo?
- Tolerância de tempo de encaminhamento - Quantos quadros são perdidos em cada roaming?

Uma impressora não se move muito, portanto os requisitos de roaming são menores. Um WGB montado no trem, por outro lado, precisa de ajuste fino no componente de roaming para garantir o comportamento correto enquanto ele se movimenta.

Um fluxo de vídeo pode ter uma grande necessidade de largura de banda, portanto, precisa de altas taxas de dados sem fio. No entanto, um aplicativo de telemetria pode precisar apenas de alguns quadros de tempos em tempos.

Éimportante que os requisitos sejam adequadamente definidos desde o início, pois afetam não apenas a configuração da WGB, mas também como a infraestrutura sem fio deve ser projetada. Por exemplo, colocação de AP, distância, níveis de energia, taxas habilitadas etc., todos afetam as características de roaming. Portanto, todos são um ponto crucial se for necessário roaming de alta velocidade.

Em geral, você deve saber estes detalhes:

- Qual é a largura de banda necessária para o aplicativo?
- Qual é a tolerância de atraso de roaming?

- O aplicativo pode lidar adequadamente com as desconexões de rede? Há um mecanismo de backup adicional?
- O aplicativo pode lidar com a perda de pacotes corretamente? (Mesmo no melhor projeto sem fio, você deve esperar uma porcentagem de perda de pacotes.)

Este documento não aborda os detalhes sobre como projetar um ambiente de RF para roaming/externo de alta velocidade. Consulte o guia de implantação de malha externa.

Roaming

Para um dispositivo sem fio, o roaming é uma parte muito crítica de sua funcionalidade.

Basicamente, roaming significa a capacidade de ir de um AP a outro, ambos pertencentes à mesma infraestrutura sem fio.

Como o roaming precisa de uma alteração do AP atual para o próximo, há uma desconexão resultante ou um tempo sem serviço. Essa desconexão pode ser pequena. Por exemplo, menos de 200 ms em implantações de voz ou muito mais tempo, mesmo segundos, se a segurança necessária impor uma autenticação completa em cada evento de roaming.

O roaming é necessário para que o dispositivo possa encontrar um novo pai com um sinal que esperamos seja melhor e possa continuar a acessar a infraestrutura de rede corretamente. Ao mesmo tempo, muitos roaming podem causar várias desconexões ou tempo sem serviço, o que afeta o acesso. É importante que um dispositivo móvel, como um WGB, tenha um bom algoritmo de roaming com recursos de configuração suficientes para se adaptar a diferentes ambientes de RF e necessidades de dados.

Elementos do roaming

- **Acionadores:** Cada implementação de cliente tem um ou mais disparadores ou eventos que, quando encontrados, fazem com que o dispositivo se mova para outro AP pai. Examples: perda de beacon (o dispositivo não ouve mais os beacons regulares do AP), novas tentativas de pacote, nível de sinal, nenhum dado recebido, quadro de desautenticação recebido, baixa taxa de dados em uso, etc. Os possíveis disparadores podem ser diferentes da implementação do cliente para outro porque não estão totalmente padronizados. Dispositivos mais simples podem ter um gatilho ruim, o que causa ruins (clientes aderentes) ou ruínas desnecessárias. O WGB suporta todos os elementos anteriores descritos anteriormente.
- **Tempo de pesquisa:** O dispositivo sem fio (WGB) passa algum tempo procurando pais em potencial. Isso normalmente implica usar canais diferentes, fazer sondagem ativa ou ouvir passivamente os APs. Como o rádio precisa fazer uma varredura, isso significa que o WGB gasta fazendo algo diferente do encaminhamento de dados. A partir desse tempo de verificação, o WGB pode criar um conjunto válido de pais para os quais o roaming pode ser feito.
- **Seleção pai:** Após o tempo de verificação, o WGB pode verificar os pais em potencial, selecionar o melhor e acionar o processo de associação/autenticação. Às vezes, o ponto de decisão pode ser permanecer no pai atual se não houver um benefício significativo de um evento de roaming (lembre-se de que o roaming demais pode ser ruim).
- **Associação/Autenticação:** O WGB continua a se associar ao novo AP, que normalmente cobre as fases de autenticação e associação do 802.11, além de concluir a política de

segurança configurada no SSID (WPA 2-PSK, CCKM, None, etc.).
- **Restauração de encaminhamento de tráfego:** O WGB atualiza a infraestrutura de rede de seus clientes com fio conhecidos por meio de atualizações do IAPP após o roaming. Depois desse ponto, o tráfego de/para os clientes com fio até a rede é retomado.

Guia de configuração - Políticas de segurança

Um aspecto importante do roaming em dispositivos móveis é a política de segurança que será implementada na infraestrutura. Há várias opções, cada uma com pontos bons/ruins. Estes são os mais importantes:

- **Aberto** — basicamente sem segurança. Esta é a política mais rápida e mais simples de todas. Este fato tem como principal problema não restringir o acesso não autorizado à infraestrutura e não proteger contra ataques, o que limita a sua utilização a cenários muito específicos. Por exemplo, minas onde não são possíveis ataques externos devido à natureza pura da implantação.
- **Autenticação de endereço MAC** —Basicamente o mesmo nível de segurança que o aberto, já que a falsificação de endereço MAC é um ataque trivial. Não recomendado devido ao tempo adicional para concluir a validação de MAC, o que retarda o roaming.
- **WPA2-PSK** — Oferece um bom nível de criptografia (AES-CCMP), mas a segurança da autenticação depende da qualidade da chave pré-compartilhada. Para medidas de segurança, recomenda-se uma senha com no mínimo 12 caracteres e aleatória. Semelhante ao método de chave pré-compartilhada, à medida que a chave é usada em vários dispositivos, se a chave for comprometida, a senha precisará ser modificada em todos os equipamentos. A velocidade de roaming é aceitável, como é feito em 6 trocas de quadros, e você pode calcular quais serão os limites de tempo superior/inferior para sua conclusão, pois ela não envolve nenhum equipamento externo (nenhum servidor RADIUS, etc.). Em geral, esse método é o preferido depois de equilibrar problemas e benefícios.
- **WPA2 com 802.1x** — Isso melhora o método anterior usando uma credencial por dispositivo/usuário, que pode ser alterada individualmente. O principal problema é que para o roaming, esse método não funciona corretamente quando o dispositivo está se movendo rápido ou são necessários tempos de roaming curtos. Em geral, ele usa os mesmos 6 quadros mais a troca EAP que pode ser entre 4 e acima. Isso depende do tipo de EAP selecionado e do tamanho do certificado. Normalmente, isso leva de 10 a 20 quadros, mais o atraso adicional no processamento do servidor radius.
- **WPA2+CCKM**—Este mecanismo oferece boa proteção, usa 802.1x para criar a autenticação inicial e, em seguida, faz uma troca rápida de apenas 2 quadros em cada evento de roaming. Isso oferece um tempo de roaming muito rápido. O principal problema é que no caso de um roaming com falha, ele reverte em 802.1x. Em seguida, começa a usar o CCKM novamente após a autenticação. Se o aplicativo sobre o WGB puder tolerar um tempo de roaming ocasional longo em caso de problemas, ele pode ser usado como a melhor opção em relação à PSK.

Este documento não aborda tecnologias não recomendadas que tenham problemas de segurança como LEAP, WPA-TKIP, WEP, etc.

Configurando WPA2-PSK

No WGB, é bastante simples de configurar. Você precisa da definição de SSID e da criptografia apropriada no rádio.

```
dot11 ssid wgbpsk
vlan 32
authentication open
authentication key-management wpa version 2
wpa-psk ascii YourReallySecurePSK!
no ids mfp client

interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

Seu nome SSID e chave pré-compartilhada devem corresponder à sua infraestrutura de rede.

Configuração do WPA2 com 802.1x

Basicamente, ele é construído sobre a configuração anterior, com a adição de perfis EAP e método de autenticação:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
!--- This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb
!--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

Configuração de WPA2 com CCKM

Apenas uma etapa na parte superior da WPA2 com apenas uma alteração secundária: usando o sinalizador CCKM na configuração do SSID. Isso pressupõe que a WLAN esteja configurada para CCKM somente no lado da WLC:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

Validação do método utilizado

Uma verificação rápida no WGB pode relatar a criptografia e o gerenciamento de chaves em uso, por exemplo, no CCKM:

```
wgb-1260#sh dot11 associations al
Address            : 0024.97f2.75a0     Name              : lap1140-etsi-1
IP Address         : 192.168.40.10      Interface         : Dot11Radio 0
Device             : LWAPP-Parent      Software Version : NONE
CCX Version        : 5                  Client MFP        : Off

State              : EAP-Assoc          Parent            : -
SSID               : wlan1
VLAN               : 0
Hops to Infra      : 0                  Association Id    : 1
Tunnel Address     : 0.0.0.0
Key Mgmt type      : CCKM               Encryption        : AES-CCMP

Current Rate       : m7.-               Capability        : WMM ShortHdr ShortSlot
Supported Rates    : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates        : disabled           Bandwidth         : 20 MHz
Signal Strength    : -59  dBm           Connected for     : 72 seconds
Signal to Noise    : 41  dB            Activity Timeout : 8 seconds
Power-save         : Off                Last Activity     : 7 seconds ago
Apsd DE AC(s)      : NONE

Packets Input      : 12064              Packets Output    : 136
Bytes Input        : 2892798            Bytes Output      : 19514
Duplicates Rcvd    : 87                 Data Retries      : 8
Decrypt Failed     : 0                  RTS Retries       : 0
MIC Failed         : 0                  MIC Missing       : 0
Packets Redirected: 0                   Redirect Filtered: 0
```

Configurando roaming

No WGB, você pode modificar vários parâmetros que afetam o algoritmo de roaming.

Tentativas de pacote

Por padrão, o WGB retransmite um quadro 64 vezes. Se não for corretamente reconhecido (ACK) por um pai, ele assumirá que o pai não é mais válido e iniciará um processo de digitalização/roaming. Veja este como um gatilho de roaming "assíncrono" porque pode ser feito a qualquer momento em que uma transmissão falha.

O comando para configurar isso, entra na interface dot11 e usa as seguintes opções:

```
packet retries NUM [drop]
```

Nº: É entre 1 e 128, com um padrão de 64. Um bom número para um gatilho de roaming rápido é geralmente 32. Não é aconselhável usar um número mais baixo na maioria dos ambientes de RF.

queda: Se não estiver presente, o WGB inicia um evento de roaming quando o máximo de novas tentativas é atingido. Quando presente, o WGB não inicia o roaming novo e usa outros disparadores, como perda e sinal de beacon.

Monitoramento de RSSI

O WGB pode implementar uma varredura de sinal pró-ativa para o pai atual e iniciar um novo processo de roaming quando o sinal cair abaixo do nível esperado.

Esse processo requer dois parâmetros:

- Um temporizador, que ativa o processo de verificação a cada X segundos
- Nível RSSI, que é usado para iniciar um processo de roaming se o sinal atual estiver abaixo dele.

Por exemplo:

```
in d0
mobile station period 4 threshold 75
```

O tempo não deve ser menor do que o que o WGB leva para concluir um processo de autenticação para impedir um "loop de roaming" em algumas condições ou para evitar um comportamento de roaming muito agressivo. Em geral, deve ser testado para ver o que acomoda as necessidades do aplicativo.

Para a PSK, ela pode ser menor do que nos métodos baseados em EAP (típicos 2 e 4 para aplicativos muito agressivos).

O nível RSSI é expresso como um inteiro positivo, embora seja basicamente um nível medido - dBm normal. Você deve usar um número ligeiramente maior do que o mínimo necessário para manter sua taxa de dados funcionando corretamente. Por exemplo, se sua taxa mínima desejada for de 6 mbps, um RSSI de limite de -87 deverá ser suficiente. Para 48 mbps, você precisa de -70 dBm, etc.

Observação: esse comando também pode disparar um "roaming por alteração na taxa de dados", que é muito agressivo. Deve ser utilizado juntamente com uma taxa mínima para obter bons resultados.

Taxa de dados mínima

Começando com 12.4(25d)JA, a Cisco adicionou um parâmetro configurável para controlar quando o WGB deve disparar um novo evento de roaming, se a taxa de dados atual para o pai estiver abaixo de um determinado valor.

Isso é útil para garantir que um limite inferior desejado de velocidade seja mantido para suportar aplicativos de vídeo ou voz.

Antes desse comando estar disponível, o WGB acionou um roaming frequentemente quando a taxa foi encontrada menor que a hora anterior. Basicamente no tempo X+1, se a taxa era menor que o tempo X anterior, o WGB iniciou um processo de roaming. Nos registros, você veria estas mensagens:

```
*Mar  1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower
data rate
```

Isso é muito agressivo e, normalmente, a única solução era configurar uma única taxa de dados em WGB e em APs pai.

Agora, a maneira recomendada é sempre configurar esse comando, sempre que um comando mobile station period é usado:

```
in d0
```

```
mobile station  minimum-rate 2.0
```
Com isso, o novo processo de roaming só será acionado se a taxa atual for inferior ao valor configurado. Isso reduz os roaming desnecessários e permite manter um valor de taxa esperado.

Observação: a mensagem `"Tive que reduzir a taxa de dados"` deve ocorrer mesmo com essa configuração, apenas que agora ela só deve ser vista se WGB foi TX em uma velocidade inferior à configurada, quando o tempo de verificação do período da estação móvel foi disparado.

Canais de varredura

O WGB verifica todos os "canais do país" enquanto realiza um evento de roaming. Isso significa que, dependendo do domínio de rádio, você pode verificar os canais de 1 a 11 em uma banda de 2,4 GHz ou de 1 a 13.

Cada canal digitalizado leva algum tempo. No 802.11bg isso é em torno de 10 a 13 ms. No 802.11a, pode ser até 150 ms se o canal estiver habilitado para DFS (portanto, não sondagem, fazendo apenas uma varredura passiva lá).

Uma boa otimização é restringir os canais digitalizados a usar apenas os que estão em serviço pela infraestrutura. Isso é especialmente importante no 802.11a, pois a lista de canais é grande, e o tempo por canal pode ser longo se o DFS estiver em uso.

Há três pontos a considerar ao projetar um plano de canal para WGB/roaming:

- Para banda de 2,4 GHz, tente aderir a 1/6/11 para minimizar a interferência lateral do canal. Qualquer outro plano de canal com 4, etc., tende a ser difícil de projetar corretamente do ponto de vista de RF, sem aumentar a interferência.
- Usar uma configuração de canal único para todos os APs é uma boa ideia do ponto de vista da digitalização. Isso só faz sentido se o número total de clientes a serem suportados for muito baixo e não houver requisitos de largura de banda altos. Isso elimina o tempo de alteração de rádio do tempo de digitalização. Esteja ciente de que poucos ambientes podem se beneficiar com essa opção, portanto, use com cuidado.
- Para a banda de 5,0 GHz, se for possível através dos regulamentos locais, utilizar canais não DFS internos (36 a 48) permite um tempo de verificação mais rápido, uma vez que o WGB pode investigar cada um de forma ativa, em vez de fazer escuta passiva por mais tempo.

O plano de canal em uso para sua implantação pode precisar acomodar outros requisitos. Use as recomendações gerais de projeto de RF.

Para configurar a lista de canais de digitalização:

```
in d0
mobile station scan 1 6 11
```
Observação: a estação móvel aparece somente quando a função WGB é usada no rádio.

Observação: certifique-se de que sua lista de verificação WGB corresponda à sua lista de canais de infraestrutura. Caso contrário, o WGB não encontrará seus APs disponíveis.

Configurar temporizadores

Começando com 12.4(25a)JA, há vários novos comandos para otimizar o temporizador de

recuperação quando um problema é encontrado, que só estão disponíveis quando o AP está no modo WGB.

```
wgb-1260(config)#workgroup-bridge timeouts ?

  assoc-response  Association Response time-out value
  auth-response   Authentication Response time-out value
  client-add      client-add time-out value
  eap-timeout     EAP Timeout value
  iapp-refresh    IAPP Refresh time-out value
```

No caso de resposta assoc, resposta automática, adição de cliente, isso indica por quanto tempo o WGB esperará a resposta do AP pai, antes de considerar o AP como inativo e tentar o próximo candidato. Os valores padrão são 5 segundos, o que é muito longo para alguns aplicativos. O temporizador mínimo é de 800 ms e é recomendado para a maioria dos aplicativos móveis.

Em eap-timeout, o WGB define um tempo máximo de espera, até que o processo de autenticação EAP completo seja concluído. Isso funciona do ponto de vista do requerente do EAP para reiniciar o processo se o autenticador do EAP não estiver respondendo. O valor padrão é de 60 segundos. Tenha cuidado para nunca configurar um valor que possa ser inferior ao tempo real necessário para concluir uma autenticação 802.1x completa. Normalmente, a definição para 2 a 4 segundos está correta para a maioria das implantações.

Para atualização de iapp, o WGB por padrão gera uma atualização em massa do IAPP para o AP pai após o roaming para informar os clientes com fio conhecidos. Há uma segunda retransmissão após a associação cerca de 10 segundos depois. Esse temporizador permite fazer uma "repetição rápida" do volume IAPP após a associação para superar a possibilidade de que a primeira atualização IAPP tenha sido perdida devido a RF ou chaves de criptografia ainda não instaladas no AP pai. Para cenários de roaming rápido, podem ser usados 100 ms. No entanto, certifique-se de que há um grande número de WGB em uso. Isso aumenta significativamente o número total de IAPP enviados à infraestrutura após cada roaming.

Exemplo de valores agregados:

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

Eles foram testados com sucesso em cenários de implantação de WGB móvel.

Outras otimizações de WGB

Há outras pequenas alterações a serem consideradas nos cenários de implantação de WGB:

Relacionado ao rádio

- Reduce **rts retries** - **rts retries 32**. Isso pode economizar um pouco de tempo de RF em cenários agressivos. Normalmente, isso não é necessário.
- Tipo de antena: Se estiver usando uma única antena (sem diversidade), você deverá configurar o rádio para melhorar o desempenho geral:

```
antenna transmit right-a
antenna receive right-a
```

A diversidade de antenas é desejável, mas nem sempre possível ao instalar fisicamente as antenas no veículo. A seleção adequada da antena é essencial para o roaming. O mínimo de 2 dB pode ser uma grande diferença nos tempos médios de roaming geral.

Log Relacionado

- Para salvar alguns milissegundos, reduza o nível de log do console para apenas erros: **logging console errors**. Não desative-o completamente porque pode afetar negativamente o desempenho do roaming em algumas condições.
- Idealmente, use telnet ou ssh do lado ethernet para coletar depurações ou registros. Isso tem um impacto muito menor no desempenho em comparação ao registro de depurações no console: **logging monitor debugging**.
- O comando para entender o que está ocorrendo para o ponto de vista de roaming WGB é **debug dot11 dot11 0 trace print uplink**. Isso tem baixo impacto na CPU, mas não ativa outras opções de depuração, a menos que seja instruído, pois cada uma pode aumentar o tempo total de roaming.
- Tente usar o SNTP quando possível. Isso mantém o tempo de sincronização do WGB, o que é extremamente útil para a solução de problemas.

uso de MFP

- O MFP pode ser útil do ponto de vista da segurança. No entanto, uma desvantagem é que em cenários de falha de roaming, o WGB não aceita quadros de desautenticação do pai do AP para disparar um novo roaming se a chave de criptografia entre ambos tiver dado errado por qualquer motivo.
- Nesses raros cenários de falha, o WGB pode levar até 5 segundos para disparar uma nova verificação, se o pai atual puder ser ouvido com um bom sinal de RF. Há um mecanismo de detecção "catch-all" que o WGB pode acionar se nenhum quadro de dados válido for recebido durante esse período.
- Por padrão, o WGB tenta usar o MFP do cliente se o SSID tiver WPA2 AES em uso.
- Recomenda-se desativar o MFP do cliente se forem necessários tempos de recuperação rápidos (WGB para reagir a quadros de áudio não protegidos). Esse é um compromisso entre as necessidades de segurança e os tempos de recuperação rápidos. A decisão depende do que é mais importante para o cenário de implantação.

```
dot11 ssid wgbpsk
   no ids mfp client
```

EAP-TLS em WGB e "intervalo de salvamento de relógio"

Consulte a seção Sincronizar Relógios Suplicantes do IOS e Configuração de Tempo para NVRAM das Notas de Versão para Pontos de Acesso Cisco Aironet e Bridges para Cisco IOS versão 12.4(21a)JY.

Lembre-se de que se estiver usando o uWGB, o uWGB talvez nunca tenha a chance de fazer uma sincronização sntp porque ela é normalmente associada ao endereço MAC conectado e o

uWGB BVI não tem acesso à rede. Portanto, no caso de um uWGB, recomenda-se obter uma boa sincronização de relógio na NVRAM, no mínimo, na implantação. Se o dispositivo enet anexado tiver a capacidade de ser uma origem NTP (assim como um cliente atualizado através da sua conexão uWGB), então é possível considerar ter a sincronização sntp uWGB a partir dela como um ponto de reflexão NTP eficaz.

Exemplo de configuração completa

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
!
dot11 syslog
!
!
dot11 ssid wgbpsk
   vlan 32
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 7 060506324F41584B56
   no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
!
antenna transmit right-a
antenna receive right-a
  packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
```

```
!

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
interface BVI1
ip address 192.168.32.67 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip

sntp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

Análise de Depuração

Em qualquer problema, é importante capturar a saída do comando **debug dot11 dot11 0 trace print uplink** como primeiro passo. Isso fornece uma boa visão do que está ocorrendo com o processo de roaming.

Este é um exemplo de pai atual como candidato:

```
 Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength
too low
 Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

Este é o disparador para um sinal baixo. Depende do comando Y threshold X da estação móvel. A primeira mensagem é sempre enviada ao console, a segunda é parte dos rastreamentos de depuração do uplink. Não é um problema, mas parte do processo WGB normal.

```
 Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

O processo Uplink força uma limpeza de fila de rádio antes de iniciar uma verificação de canal. Essa etapa pode levar de alguns milissegundos a vários segundos, dependendo da utilização do canal e da profundidade da fila. Os quadros de dados não têm tempo limite. Os quadros de voz têm uma comparação de tempo feita, portanto devem ser descartados mais rápido. Algum atraso pode ser observado em ambientes ruidosos.

```
 Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
 Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

Esta é a análise de canal real que está a ocorrer. Ele estaciona o rádio aproximadamente de 10 a 13 ms por canal configurado.

```
 Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

Esta é a lista de respostas de sondagem recebidas. O primeiro número é o canal, o segundo são microssegundos usados para recebê-lo.

```
 Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0,
load 0
 Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0,
load 0
```

Comparação real feita nestes detalhes:

```
 Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet
```

Seleção pai

```
 Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done
 Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0,
 Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed.
```

Este é o ponto onde o roaming está "terminado". O tráfego é retomado assim que os quadros IAPP são processados pelo pai.

Informações de comparação pai

```
 Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0,
load 3
 Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1,
load 0
```

O compare1 imprime a contagem de associação real -1 (portanto, o próprio WGB não é tomado no número) se o AP "atual" ainda for o WGB associado, depois saltos reais e carga.

O compare2 imprime as diferenças. Por isso é possível ver um número negativo. Se o teste tiver um número maior que a corrente, você verá negativo.

Dependendo da contagem de associação atual, carga, diferença de sinal, valor de limite móvel, o WGB pode ou não selecionar um novo pai.

A comparação é sempre entre dois APs, com o AP selecionado substituindo a corrente para a próxima iteração. Portanto, algumas das decisões podem ser devido ao RSSI em um loop ou devido a outros fatores no próximo teste.

Informações Relacionadas

- Como usar o aIOS WGB com autenticação EAP-TLS em uma Cisco Unified Wireless Network
- Suporte Técnico e Documentação - Cisco Systems