Roaming WGB: Detalles internos y configuración

Contenido

Introducción

Cisco Workgroup Bridge (WGB) es una herramienta muy útil para el diseño e implementación de una red inalámbrica, ya que permite que los dispositivos no inalámbricos adquieran movilidad. WGB proporciona muchos detalles sobre la itinerancia, el acceso a la seguridad, etc., que afectan a los escenarios de implementación en función de sus necesidades.

En las versiones de código 12.4(25d)JA y posteriores, Cisco introdujo un conjunto de comandos y cambios para optimizar el uso de WGB en entornos de roaming de alta velocidad.

Este documento cubre diferentes aspectos de cómo funciona un WGB, incluidos los puntos de decisión del algoritmo de roaming, y cómo configurarlo para el modelo de uso esperado.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Solución de LAN inalámbrica de Cisco
- Puente de grupo de trabajo de Cisco

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

¿Qué es un puente de grupo de trabajo?

Un WGB es básicamente un punto de acceso (AP) configurado para actuar como cliente inalámbrico hacia una infraestructura y para proporcionar conectividad de Capa 2 para los dispositivos conectados a su interfaz Ethernet.

Una implementación típica de WGB tiene estos componentes:

- dispositivo WGB, normalmente con al menos una interfaz de radio y una interfaz Ethernet
- Una infraestructura inalámbrica, normalmente denominada AP raíz, que puede ser autónoma o unificada.
- Uno o más dispositivos cliente con cables conectados al WGB. Este documento no cubre escenarios de rol mixtos (una radio como WGB, una radio como raíz en el mismo AP).

Hay tres tipos principales de WGB:

- **WGB de Cisco**: Cisco WGB es cualquier punto de acceso basado en Cisco IOS® configurado como WGB (1130, 1240, 1250, etc). Este modo utiliza el protocolo IAPP para informar a la infraestructura de red de los dispositivos que el WGB ha aprendido en su interfaz Ethernet. En este caso, el controlador de LAN inalámbrica (WLC) o el AP raíz tienen visibilidad de Capa 2 de los dispositivos "colgando" del WGB.
- **WGB que no es de Cisco:** Se trata de un dispositivo de terceros que actúa como WGB y conecta uno o varios dispositivos con cables a la infraestructura inalámbrica. Estos no

admiten IAPP, y permiten solamente un único dispositivo con cables, o proporcionan un mecanismo de traducción de direcciones MAC, ocultando a todos sus clientes con cables detrás de una única dirección MAC 802.11. Estos tipos de dispositivos necesitan un manejo especial en las tramas DHCP y del protocolo de resolución de direcciones (ARP) si la infraestructura es un WLC debido a las verificaciones de seguridad y el manejo de tramas realizado en los controladores.
- **Cisco AP configurado como "WGB universal"**: Este es un modo que suprime el mecanismo IAPP, de modo que el WGB se puede utilizar hacia una infraestructura de Cisco o hacia AP raíz de terceros. En este caso, el WGB toma la dirección de su cliente Ethernet, limitando el número de dispositivos detrás de él a uno.

La siguiente sección se centra en el escenario de un WGB de Cisco utilizado hacia una infraestructura autónoma o WLC.

Escenarios de uso

Los ejemplos de uso típicos de WGB incluyen:

- Conexión de una impresora con cables a la red
- Diferentes implementaciones de fabricación, en las que no es factible ni práctico ejecutar un cable en el dispositivo por cable
- Implementaciones en vehículos, donde el WGB proporciona conectividad desde un coche, metro, etc., a una red inalámbrica exterior
- Cámaras con cables

Cada ejemplo tiene sus propios requisitos en términos de:

- Ancho de banda necesario para admitir la aplicación que se ejecutará sobre la infraestructura inalámbrica
- Tolerancia de retardo de roaming: ¿Cuánto tiempo tarda el WGB en pasar del AP actual al siguiente mientras el dispositivo se mueve?
- Tolerancia de tiempo de reenvío: ¿cuántas tramas se pierden en cada roaming?

Una impresora no se mueve mucho, por lo que los requisitos de itinerancia son más bajos. Por otra parte, un tren montado en WGB necesita un ajuste fino en el componente de roaming para asegurar un comportamiento correcto mientras se mueve.

Una secuencia de vídeo puede tener un gran ancho de banda necesario, por lo que necesita altas velocidades de datos inalámbricos. Sin embargo, es posible que una aplicación de telemetría sólo necesite algunas tramas de vez en cuando.

Es importante que los requisitos se definan correctamente desde el principio, ya que afectan no sólo a la configuración del WGB, sino también a cómo se debe diseñar la infraestructura inalámbrica. Por ejemplo, la ubicación de AP, la distancia, los niveles de potencia, las velocidades habilitadas, etc., afectan todas las características de itinerancia. Por lo tanto, todos son un punto crucial si se necesita una itinerancia de alta velocidad.

En general, debe conocer estos detalles:

- ¿Cuál es el ancho de banda necesario para la aplicación?
- ¿Cuál es la tolerancia de demora de roaming?
- ¿La aplicación puede manejar las desconexiones de red correctamente? ¿Hay algún

mecanismo de respaldo adicional?
- ¿La aplicación puede manejar la pérdida de paquetes correctamente? (Incluso en el mejor diseño inalámbrico, debe esperar un porcentaje de pérdida de paquetes).

Este documento no trata los detalles sobre cómo diseñar un entorno RF para roaming/exterior de alta velocidad. Consulte la guía de implementación de malla exterior.

Roaming

Para un dispositivo inalámbrico, la itinerancia es una parte muy importante de su funcionalidad.

Básicamente, roaming significa la capacidad de ir de un AP a otro, ambos pertenecientes a la misma infraestructura inalámbrica.

Como la itinerancia necesita un cambio del AP actual al siguiente, hay una desconexión resultante o tiempo sin servicio. Esta desconexión puede ser pequeña. Por ejemplo, menos de 200 ms en implementaciones de voz o mucho más, incluso segundos, si la seguridad necesita aplicar una autenticación completa en cada evento de roaming.

La itinerancia es necesaria para que el dispositivo pueda encontrar un nuevo dispositivo principal con una mejor señal y pueda continuar accediendo a la infraestructura de red correctamente. Al mismo tiempo, demasiados itinerarios pueden provocar varias desconexiones o tiempo sin servicio, lo que afecta al acceso. Es importante que un dispositivo móvil, como un WGB, tenga un buen algoritmo de itinerancia con suficientes capacidades de configuración para adaptarse a diferentes entornos de RF y necesidades de datos.

Elementos de roaming

- **Desencadenadores:** Cada implementación del cliente tiene uno o más desencadenadores o eventos que, cuando se encuentran, hacen que el dispositivo se mueva a otro AP primario. Examples: pérdida de baliza (el dispositivo ya no oye las balizas regulares del AP), reintentos de paquetes, nivel de señal, no se reciben datos, trama de desautenticación recibida, baja velocidad de datos en uso, etc. Los posibles desencadenadores pueden ser diferentes de la implementación del cliente a otro porque no están completamente estandarizados. Los dispositivos más sencillos podrían tener un conjunto de disparadores deficiente, lo que podría provocar problemas (clientes pegajosos) o desplazamientos innecesarios. El WGB admite todos los elementos anteriores descritos anteriormente.
- **Tiempo de análisis:** El dispositivo inalámbrico (WGB) dedica algún tiempo a buscar posibles padres. Esto normalmente implica ir a diferentes canales, hacer sondeo activo o escuchar pasivamente los AP. Como la radio tiene que escanear, esto significa el tiempo que el WGB gasta en hacer algo diferente de reenviar datos. A partir de este tiempo de escaneo, el WGB puede crear un conjunto válido de padres a los que se pueda trasladar.
- **Selección principal:** Después del tiempo de escaneo, el WGB puede verificar los padres potenciales, seleccionar el mejor y activar el proceso de asociación/autenticación. A veces, el punto de decisión puede ser permanecer en el padre actual si no hay un beneficio significativo de un evento de roaming (recuerde que el roaming demasiado puede ser malo).
- **Asociación/Autenticación:** El WGB procede a asociarse al nuevo AP, que normalmente cubre las fases de autenticación y asociación 802.11, además de completar la política de seguridad configurada en el SSID (WPA 2-PSK, CCKM, None, etc.).

- **Restauración de reenvío de tráfico:** El WGB actualiza la infraestructura de red de sus clientes conocidos por cable a través de las actualizaciones de IAPP después de la itinerancia. Después de este punto, se reanuda el tráfico hacia/desde los clientes cableados a la red.

Guía de configuración - Políticas de seguridad

Un aspecto importante de la itinerancia en los dispositivos móviles es la política de seguridad que se implementará en la infraestructura. Hay varias opciones, cada una con puntos buenos o malos. Estos son los más importantes:

- **Abrir**: básicamente no hay seguridad. Esta es la más rápida y simple de todas las políticas. Esto plantea el principal problema de no restringir el acceso no autorizado a la infraestructura y de no proteger contra ataques, lo que limita su uso a escenarios muy específicos. Por ejemplo, las minas en las que no es posible realizar ataques externos debido a la naturaleza del despliegue.
- **Autenticación de dirección MAC**: básicamente, el mismo nivel de seguridad que el abierto, ya que la suplantación de dirección MAC es un ataque trivial. No se recomienda debido al tiempo agregado para completar la validación MAC, que ralentiza el roaming.
- **WPA2-PSK**: ofrece un buen nivel de encriptación (AES-CCMP), pero la seguridad de la autenticación depende de la calidad de la clave precompartida. Para las medidas de seguridad, se recomienda una contraseña de 12 caracteres como mínimo y aleatoria. Al igual que el método de clave previamente compartida, ya que la clave se utiliza en varios dispositivos, si la clave se ve comprometida, la contraseña debe modificarse en todos los equipos. La velocidad de roaming es aceptable, ya que se realiza en 6 intercambios de tramas, y puede calcular cuáles serán los límites de tiempo superior/inferior para que se complete porque no implica ningún equipo externo (no hay servidor RADIUS, etc). En general, este método es el preferido después de equilibrar problemas y beneficios.
- **WPA2 con 802.1x**: esto mejora el método anterior al utilizar una credencial por dispositivo/usuario, que se puede cambiar individualmente. El problema principal es que para el roaming, este método no funciona correctamente cuando el dispositivo se mueve rápido o se necesitan tiempos de itinerancia cortos. En general, esto utiliza las mismas 6 tramas más el intercambio EAP que puede estar entre 4 y superior. Esto depende del tipo de EAP seleccionado y del tamaño del certificado. Normalmente, esto toma entre 10 y 20 tramas, más el retraso agregado del procesamiento del servidor RADIUS.
- **WPA2+CCKM**: este mecanismo ofrece una buena protección, utiliza 802.1x para generar la autenticación inicial y, a continuación, realiza un intercambio rápido de sólo 2 tramas en cada evento de roaming. Esto ofrece un tiempo de roaming muy rápido. El problema principal es que en el caso de una vagina fallida, vuelve a funcionar en 802.1x. A continuación, comienza a utilizar CCKM de nuevo después de autenticarse. Si la aplicación en la parte superior del WGB puede tolerar un tiempo de roaming largo ocasional en caso de problemas, se puede utilizar como la mejor opción frente a PSK.

Este documento no cubre las tecnologías no recomendadas que tienen problemas de seguridad como LEAP, WPA-TKIP, WEP, etc.

Configuración de WPA2-PSK

En el WGB, esto es bastante simple de configurar. Necesita una definición SSID y el cifrado

adecuado en la radio.

```
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
```

El nombre SSID y la clave previamente compartida deben coincidir con su infraestructura de red.

Configuración de WPA2 con 802.1x

Básicamente se basa en la configuración anterior, con la adición de perfiles EAP y método de autenticación:

```
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
```

Configuración de WPA2 con CCKM

Solo hay un paso por encima de WPA2 con un cambio menor: utilizando el indicador CCKM en la configuración SSID. Esto supone que la WLAN se configura para CCKM solamente en el lado del 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
```

Validación del método utilizado

Una comprobación rápida del WGB puede informar de la administración de claves y cifrado en uso, por ejemplo, en 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
```

Configuración de Roaming

En el WGB, puede modificar varios parámetros que afectan al algoritmo de roaming.

Reintentos de paquetes

De forma predeterminada, el WGB retransmite una trama 64 veces. Si un padre no reconoce correctamente (ACK), supone que el padre ya no es válido e inicia un proceso de exploración/itinerancia. Vea este como un disparador de roaming "asíncrono" porque se puede hacer en cualquier momento que falla una transmisión.

El comando para configurar esto, entra en la interfaz dot11 y toma las siguientes opciones:

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

Num: Está entre 1 y 128, con un valor predeterminado de 64. Un buen número para un disparador de roaming rápido es generalmente 32. El uso de un número menor no es recomendable en la mayoría de los entornos de RF.

descartar: Si no está presente, el WGB inicia un evento de roaming cuando se alcanzan los reintentos máximos. Cuando está presente, el WGB no inicia el nuevo roaming y utiliza otros desencadenadores, como la pérdida de baliza y la señal.

Supervisión de RSSI

WGB puede implementar un escaneo de señal proactivo para el padre actual e iniciar un nuevo proceso de roaming cuando la señal cae por debajo del nivel esperado.

Este proceso toma dos parámetros:

- Un temporizador, que activa el proceso de verificación cada X segundos
- Nivel RSSI, que se utiliza para iniciar un proceso de roaming si la señal actual está por debajo de él.

Por ejemplo:

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

El tiempo no debería ser menor que lo que el WGB necesita para completar un proceso de autenticación para evitar un "loop de roaming" en algunas condiciones o para evitar un comportamiento de roaming demasiado agresivo. En general, debe probarse para comprobar qué satisface las necesidades de la aplicación.

Para PSK puede ser inferior que en los métodos basados en EAP (típicos 2 y 4 para aplicaciones muy agresivas).

El nivel RSSI se expresa como un entero positivo, aunque es básicamente un nivel normal medido -dBm. Debe utilizar un número ligeramente superior al mínimo necesario para mantener la velocidad de datos en funcionamiento correctamente. Por ejemplo, si la velocidad mínima deseada es de 6 mbps, un RSSI de umbral de -87 debe ser suficiente. Para una potencia de 48 mbps, necesita -70 dBm, etc.

Nota: Este comando también puede activar un "roaming por cambio de velocidad de datos", que es demasiado agresivo. Debe utilizarse junto con una tasa mínima para obtener buenos resultados.

Velocidad de datos mínima

A partir de 12.4(25d)JA, Cisco agregó un parámetro configurable para controlar cuándo el WGB debe activar un nuevo evento de itinerancia, si la velocidad de datos actual a la principal es inferior a un valor determinado.

Esto es útil para asegurarse de que se mantenga una velocidad límite inferior deseada para admitir aplicaciones de vídeo o voz.

Antes de que este comando estuviera disponible, el WGB activó un roaming con frecuencia cuando se descubrió que la velocidad era menor que la anterior. Básicamente en el tiempo X+1, si la velocidad era menor que la X anterior, el WGB inició un proceso de roaming. En los registros verá estos mensajes:

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

Esto es demasiado agresivo, y normalmente, la única solución era configurar una única velocidad de datos tanto en WGB como en los AP primarios.

Ahora, la forma recomendada es configurar siempre este comando, siempre que se utilice un comando mobile station period:

```
in d0
mobile station  minimum-rate 2.0
```

Con esto, el nuevo proceso de roaming sólo se activa si la velocidad actual es inferior al valor

configurado. Esto reduce los desplazamientos innecesarios y permite mantener un valor de tasa esperado.

Nota: Se espera que el mensaje `"Tenía que reducir la velocidad de datos"` ocurra incluso con esta configuración, sólo que ahora sólo debería verse si WGB era TX a una velocidad inferior a la configurada, cuando se activó el tiempo de verificación del período de la estación móvil.

Buscar canales

El WGB escanea todos los "canales de países" mientras realiza un evento de roaming. Esto significa que, dependiendo del dominio de radio, puede escanear los canales 1 a 11 en la banda de 2,4 GHz o de 1 a 13.

Cada canal escaneado lleva algún tiempo. En 802.11bg esto es de unos 10 a 13 ms. En 802.11a, puede ser de hasta 150 ms si el canal está habilitado para DFS (por lo tanto, no sondeo, sólo escaneo pasivo allí).

Una buena optimización es restringir los canales escaneados para que utilicen solamente los que están en servicio por la infraestructura. Esto es especialmente importante en 802.11a, ya que la lista de canales es grande y el tiempo por canal puede ser largo si el DFS está en uso.

Hay tres puntos a tener en cuenta al diseñar un plan de canal para WGB/Roaming:

- Para la banda de 2,4 GHz, intente ajustarse a 1/6/11 para minimizar la interferencia del canal lateral. Cualquier otro plan de canal con 4, etc., tiende a ser difícil de diseñar adecuadamente desde el punto de vista de RF, sin aumentar las interferencias.
- El uso de una configuración de canal único para todos los AP es una buena idea desde el punto de vista del escaneo. Esto solo tiene sentido si el número total de clientes que se deben admitir es muy bajo y no hay requisitos de ancho de banda altos. Esto elimina el tiempo de cambio de radio del tiempo de escaneo. Tenga en cuenta que pocos entornos se pueden beneficiar de esta opción, por lo que debe usarse con cuidado.
- Para la banda de 5,0 GHz, si es posible gracias a las normativas locales, el uso de canales interiores no DFS(36 a 48) permite un tiempo de escaneo más rápido, ya que WGB puede sondear cada uno de ellos de forma activa, en lugar de hacer una escucha pasiva durante más tiempo.

Es posible que el plan de canal en uso para la implementación deba adaptarse a otros requisitos. Utilice las recomendaciones generales de diseño de RF.

Para configurar la lista de canales de escaneo:

```
in d0
mobile station scan 1 6 11
```

Nota: La estación móvil sólo aparece cuando se utiliza la función WGB en la radio.

Nota: Asegúrese de que la lista de exploración de WGB coincide con la lista de canales de infraestructura. Si no, el WGB no encontrará sus AP disponibles.

Configurar temporizadores

A partir de 12.4(25a)JA, hay varios comandos nuevos para optimizar el temporizador de

recuperación cuando se encuentra un problema, que sólo están disponibles cuando el AP está en 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
```

En el caso de assoc-response, auth-response, client-add, estos indican cuánto tiempo esperará el WGB para que el AP primario conteste, antes de considerar el AP como muerto el y probar siguiente candidato. Los valores predeterminados son 5 segundos, lo que es demasiado largo para algunas aplicaciones. El temporizador mínimo es de 800 ms y se recomienda para la mayoría de las aplicaciones móviles.

En eap-timeout, el WGB establece un tiempo máximo de espera hasta que se complete el proceso completo de autenticación EAP. Esto funciona desde el punto de vista del suplicante EAP para reiniciar el proceso si el autenticador EAP no responde. El valor predeterminado es 60 segundos.' Tenga cuidado de no configurar nunca un valor que pueda ser inferior al tiempo real necesario para completar una autenticación 802.1x completa. Normalmente, establecer esto en 2 a 4 segundos es correcto para la mayoría de las implementaciones.

Para actualización de iapp, el WGB genera de forma predeterminada una actualización masiva de IAPP al AP primario después de la itinerancia para informar de los clientes cableados conocidos. Hay una segunda retransmisión después de la asociación unos 10 segundos después. Este temporizador permite hacer un "reintento rápido" del IAPP masivo después de la asociación para superar la posibilidad de que la primera actualización IAPP se haya perdido debido a RF, o las claves de cifrado aún no instaladas en el AP primario. Para escenarios de itinerancia rápida, se pueden utilizar 100 ms. Sin embargo, asegúrese de que hay un gran número de WGB en uso. Esto aumenta significativamente el número total de IAPP enviadas a la infraestructura después de cada roaming.

Ejemplo para valores agresivos:

```
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
```

Estos se han probado correctamente en escenarios de implementación de WGB móviles.

Otras optimizaciones de WGB

Hay otros cambios menores que se deben tener en cuenta para los escenarios de implementación de WGB:

Relacionado con la radio

- Reduzca **los reintentos rts** - **rts retries 32**. Esto puede ahorrar algo de tiempo de RF en escenarios agresivos. Normalmente esto no es necesario.

- Tipo de antena: Si utiliza una sola antena (sin diversidad), debe configurar la radio para mejorar el rendimiento general:

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

La diversidad de la antena es deseable, pero no siempre es posible cuando se instalan físicamente antenas en el vehículo. La selección adecuada de la antena es fundamental para el roaming. Tan solo 2 dB pueden ser una gran diferencia en los tiempos promedio de roaming general.

Relacionado con el registro

- Para guardar algunos milisegundos, reduzca el nivel de registro de la consola a errores solamente: **registro de errores de consola**. No lo desactive completamente porque puede afectar negativamente al rendimiento de roaming en algunas condiciones.
- Lo ideal es utilizar telnet o ssh del lado de Ethernet para recopilar debugs o logs. Esto tiene un impacto mucho menor en el rendimiento en comparación con los debugs de registro sobre la consola: **logging monitor debugging**.
- El comando para entender lo que ocurre para el punto de vista de roaming de WGB es **debug dot11 dot11 0 trace print uplink**. Esto tiene un impacto bajo en la CPU, pero no habilite otras opciones de depuración a menos que se les indique porque cada una podría aumentar el tiempo de roaming total.
- Intente utilizar SNTP cuando sea posible. Esto mantiene el tiempo WGB sincronizado, lo que resulta extremadamente útil para la resolución de problemas.

uso de MFP

- MFP puede ser útil desde el punto de vista de la seguridad. Sin embargo, un inconveniente es que en los escenarios de falla de roaming, el WGB no acepta tramas de desautenticación del AP primario para activar un nuevo roaming si la clave de cifrado entre ambos se ha equivocado por cualquier razón.
- En estos escenarios de fallas poco comunes, el WGB puede tardar hasta 5 segundos en activar un nuevo escaneo, si el padre actual puede ser escuchado con una buena señal de RF. Hay un mecanismo de detección "catch-all" que WGB puede activar si no se reciben tramas de datos válidas durante ese tiempo.
- De forma predeterminada, el WGB intenta utilizar la MFP del cliente si el SSID tiene WPA2 AES en uso.
- Se recomienda desactivar la MFP del cliente si se necesitan tiempos de recuperación rápidos (WGB para reaccionar a las tramas de deauth no protegidas). Esto supone un riesgo entre las necesidades de seguridad y los rápidos tiempos de recuperación. La decisión depende de lo que es más importante para el escenario de implementación.

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

EAP-TLS en WGB y "intervalo de ahorro de reloj"

Consulte la sección Sincronización de los Relojes de Suplicante de IOS y Ahorro de Tiempo en

NVRAM de Release Notes para los Puntos de Acceso y Bridges Cisco Aironet para Cisco IOS Release 12.4(21a)JY.

Tenga en cuenta que si utiliza uWGB, el uWGB podría nunca tener la oportunidad de realizar una sincronización sntp porque normalmente está asociado con la dirección MAC conectada y el uWGB BVI no tiene acceso a la red. Por lo tanto, en el caso de un uWGB, se recomienda obtener una buena sincronización del reloj en NVRAM en la implementación como mínimo. Si el dispositivo de entrada conectado tiene la capacidad de ser un origen NTP (así como un cliente actualizado a través de su conexión uWGB), entonces es posible considerar tener la sincronización sntp uWGB de él como un punto de reflexión NTP efectivo.

Ejemplo de configuración 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
```

Análisis de depuración

En cualquier problema, es importante capturar el resultado del **comando debug dot11 dot11 0 trace print uplink** como primer paso. Esto proporciona una buena visión de lo que está ocurriendo con el proceso de roaming.

Este es un ejemplo de padre actual 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 es el disparador para la señal baja recibida. Depende del comando mobile station period X threshold Y. El primer mensaje siempre se envía a la consola, el segundo es parte de los seguimientos de depuración de link ascendente. No es un problema, sino parte del proceso normal de la WGB.

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

El proceso Uplink fuerza una depuración de la cola de radio antes de iniciar una exploración del canal. Este paso puede tardar de unos milisegundos a varios segundos dependiendo del uso del canal y la profundidad de la cola. No se agota el tiempo de espera de las tramas de datos. Las tramas de voz tienen una comparación de tiempo realizada, por lo que se deben descartar más rápido. Se puede observar cierta demora en entornos ruidosos.

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

Esta es la exploración del canal real que se está llevando a cabo. Aplaza la radio 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 es la lista de respuestas de sonda recibidas. El primer número es el canal, el segundo son los microsegundos que se toman para recibirlo.

```
 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
```

Comparación real realizada en estos detalles:

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

Selección principal

```
 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 es el punto en el que el roaming está "terminado". El tráfico se reanuda en cuanto las tramas IAPP son procesadas por el padre.

Información de comparación principal

```
 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
```

El comando compare1 imprime el recuento de asociación real -1 (por lo tanto, el propio WGB no se toma en el número) si el AP "actual" sigue siendo el único WGB asociado, entonces saltos reales y carga.

El comando compare2 imprime las diferencias. Por eso es posible ver un número negativo. Si la prueba tiene un número mayor que la actual, verá negativo.

En función del recuento de asociaciones, la carga, la diferencia de señal, el valor del umbral móvil, el WGB podría o no seleccionar un nuevo padre.

La comparación siempre es entre dos AP, con el AP seleccionado reemplazando la actual para la siguiente iteración. Por lo tanto, algunas de las decisiones pueden deberse a RSSI en un loop, o a otros factores en la siguiente prueba.

Información Relacionada

- Cómo Utilizar aIOS WGB con Autenticación EAP-TLS en una Red Cisco Unified Wireless
- Soporte Técnico y Documentación - Cisco Systems