Guía de diseño al aire libre de la movilidad

Contenido

Introducción

Este documento proporciona la guía para el diseño para la implementación de Infraestructura de Movilidad en exteriores. Este documento toca abreviadamente solamente los Productos relevantes que son convenientes y recomendados para las implementaciones de la movilidad en el aire libre. Para una comprensión completa de estas líneas de producto, refiera a las actualizaciones del producto respectivo en el sitio Web de Cisco o pase a través de los Guías de despliegue respectivos.

Nota: Usted necesita una imagen autónoma especial en el (APS) autónomo de los Puntos de acceso que es utilizado como el (WGB) o router de acceso móvil (MARCHA) del Work Group Bridge para la Interoperabilidad con la infraestructura unificada CAPWAP.

Los links importantes, útiles se proporcionan en el Annexure asociados en el extremo.

Las hojas de ruta (traveler) de hoy están exigiendo más seguro, seguro, y los métodos confiables de transporte para personal y las necesidades comerciales. Con la demanda creciente de la gente que se conectará dondequiera en cualquier momento, la movilidad en el aire libre usando el carril o cualquier otra infraestructura está adaptando hasta cubre estas demandas crecientes de sus pasajeros. Mientras que los teléfonos móviles pueden proporcionar una solución para las comunicaciones por voz, no han probado útil en la entrega del negocio y de las comunicaciones de datos personales que el público ha hecho acostumbrado a usar.

Para entregar un más confiable, seguro, y asegurar la solución del transporte, las operaciones del carril deben mejorar con el uso de las Tecnologías móviles. Proporcionando a de alta velocidad, las comunicaciones por teléfono móvil confiables, no sólo al tren, pero a cualquier otra infraestructura, las hojas de ruta (traveler) y los empleados pueden permanecer conectadas con su negocio y información personal.

Con millones de hojas de ruta (traveler) al año, la industria del transporte se ha estado moviendo rápidamente para ampliar y para mejorar las operaciones del carril con las Tecnologías móviles (soluciones).

Los motivadores principales del negocio para la movilidad son acceso en tiempo real a los datos contra las actualizaciones del lote, las operaciones mejoradas de la vigilancia dentro de los trenes de mudanza que ayudan en la ubicación que sigue en caso de emergencia, de costes reducidos, y de ancho de banda creciente de las comunicaciones substituyendo el uso de los links por satélite y/o celulares con los link de red inalámbrica cones base en tierra.

La arquitectura del Cisco Unified Wireless proporciona la Conectividad confiable del ancho de banda alto en los trenes de mudanza. Esta guía de diseño le ayuda a entender cómo construir tal sistema con eficacia.

Las tecnologías de red inalámbrica se diseñan usando los sistemas de radio que están conforme a interferencia de la onda de radio. Las causas de esta interferencia pueden ser accidentales o deliberadas. Sin importar la fuente, interferencia puede interrumpir la conexión de red inalámbrica, inhabilitando cualquier solución que dependa del WI-FI. Dado tales riesgos, las soluciones que afectan la seguridad pública no deben depender SOLAMENTE de las tecnologías de red

inalámbrica. Redundante, se prefieren el solapar, y los sistemas independientes (e.g atado con alambre y Tecnología inalámbrica). En el contexto de los sistemas de control del tren, los ejemplos de solapar, los sistemas redundantes incluyen, pero no se limitan a: emparejar las tecnologías de red inalámbrica con dos o más sistemas independientes, sistemas mecánicos (e.g. “Switch del deadman "), señalización de control del tren sobre los carriles metálicos, y descuido humano a bordo y central (driver del tren) o supervisores del control central. Si un sistema fallara, otro sistema independiente todavía estaría disponible, ayudando reduce los riesgos a la seguridad pública.

El despliegue de la movilidad se puede dividir en dos secciones principales. Primero está la infraestructura inmóvil en la cual el cliente de red inalámbrica de itinerancia rápido interoperará, y el segundo es la infraestructura móvil que consiste en el cliente de itinerancia sin hilos sí mismo. Hay algunos Productos de tecnología inalámbrica de Cisco específicos que tienen un conjunto de características peculiar que los hace convenientes para la movilidad.

La infraestructura inmóvil se puede crear usando los Puntos de acceso al aire libre de la malla de Cisco (mapas) (AP1520 Series). No intente crear una red de interconexión en el aire libre usando los mapas interiores (AP1130 y AP1240) pues estos AP no se construyen sólidamente para el uso al aire libre y haber limitado el poder. Utilice un MAPA interior dentro solamente.

Semejantemente, para la infraestructura de itinerancia, usted puede utilizar la tecnología inalámbrica de Cisco AP autónomos en el modo WGP, o el router de acceso móvil MAR3200 de Cisco.

Resaltarán al conjunto de características de los productos respectivos que los hacen convenientes para la movilidad en este documento.

Infraestructura inmóvil usando los mapas

Las implementaciones al aire libre también requieren las habilidades especializadas del Radiofrecuencia (RF), pueden tener una densidad más baja del usuario que las implementaciones interiores, y se pueden desplegar en un entorno que se regule menos que dentro de un edificio. La presión aplicada estas características sobre el costo total de propiedad (TCO) de las soluciones al aire libre, y requiere una solución que sea fácil de desplegar y de mantener.

La solución de interconexión de redes de la malla de la tecnología inalámbrica de Cisco habilita el despliegue rentable y seguro de la empresa, del campus, y de las redes al aire libre metropolitanas del Wi-Fi.

Los mapas de las AP1520 Series se basan en CAPWAP que actúa con el software de los controladores LAN (WLCs) y del Cisco Wireless Control System de la tecnología inalámbrica de Cisco (WCS) para proporcionar la Administración centralizada y scalable, la gran seguridad, y la movilidad que es inconsútil entre las implementaciones interiores y al aire libre.

El WLCs múltiple se puede agrupar junto en un grupo de la movilidad, de modo que todos los AP manejaran por ellos la forma un dominio de red inalámbrica solo, inconsútil. El número máximo de WLCs en un solo grupo es 24. Éste es más profundizado discutido más adelante en este documento.

La información detallada sobre los diversos reguladores y sus capacidades se puede encontrar en este link: http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html.

Diseñó soportar la facilidad de las implementaciones, el MAPA de las Cisco 1520 Series basado en CAPWAP, se une a fácilmente y con seguridad la red de interconexión, y está disponible manejar y monitorear la red a través del regulador y el WCS gráficos o el comando line interface(cli). Obediente con el Wi-Fi protegió el acceso 2 (WPA2) y empleando el cifrado basado en hardware del Advanced Encryption Standard (AES) entre los Nodos inalámbricos, el MAPA de las Cisco 1520 Series proporciona la seguridad de extremo a extremo.

AP1520 se ha certificado a IP67, las especificaciones NEMA4X, eliminando la necesidad de tener la nema adicional u otros recintos a prueba de mal tiempo y puede actuar en las temperaturas que se extendían de -40°C hasta el final a +55°C sin ninguna temperatura externa que influenciaba los dispositivos. La unidad entera se diseña para soportar y todavía actuar en las condiciones severas incluyendo el viento muy fuerte y la precipitación de todos teclea.

La plataforma AP1520 (AP1524 y AP1522) en conjunto es un diseño modular y se puede configurar con estas interfaces del link ascendente opcional:

- DOCSIS 2.0 del módem de cable con la fuente de alimentación del cable
- Interfaz de la fibra con 100BaseBX SFP
- 1000BaseT Gig Ethernet

Esta plataforma también da a salida 802.3af del PoE el puerto listo para conectar cualquier dispositivo periférico (como las cámaras).

Las 1520 Series AP soportan cuatro interfaces de Ethernet Gigabite:

- Puerto 0 (g0) - Poder sobre el puerto-PoE de la entrada de los Ethernetes (adentro)
- Puerto 1 (g1) - Poder sobre el puerto-PoE de la salida de los Ethernetes (hacia fuera)
- Puerto 2 (g2) - conexión por cable
- Puerto 3 (g3) - conexión de fibra

Interfaces en un MAPA

La plataforma AP1520 ha dado a luz a muchos mapas como AP1522, AP1524PS (seguridad pública), y AP1524SB (regreso serial).

Con 7.0 código, usted puede pedir el AP1523 CV que tiene básicamente el mismo hardware que el AP1524SB, salvo que tiene un módem de cable incorporado, similar al modelo AP1522PC-X-K9. En términos más simples, el AP1522 y el AP1523CV se pueden configurar con un módem de cable mientras que ordena, mientras que los modelos AP1524SB y AP1524PS no están disponibles con un módem de cable.

Nota: El AP1523CV está solamente disponible adentro – Un dominio con el código 7.0. En este documento, todas las funciones explicadas para el AP1524SB son también aplicables al AP1523CV.

Llega a ser importante entender las características fundamentales AP1524SB que hacen mejor conveniente para un tipo Lineal de despliegue. Sobre todo, las implementaciones de la movilidad requieren este tipo de infraestructura:

Infraestructura para las implementaciones de la movilidad

Funciones seriales del regreso AP1524 (AIR-LAP1524SB-X-K9)

Radios y canales

El AP1524 tiene tres radios: una radio 2.4 gigahertz y dos radios 5 gigahertz. Su radio 2.4 gigahertz se utiliza sobre todo para el acceso al cliente. Dos radios 5 gigahertz se utilizan sobre todo para el regreso. Estos dos regresos proporcionan un uplink y un acceso del link descendente. Guardándolos en los canales o las bandas de frecuencia exclusivos, se evita la necesidad de utilizar el mismo media inalámbrico compartido entre el tráfico del norte y en dirección sur en una red árbol-basada malla. En términos más simples, podemos decir que cada salto utiliza una diversa frecuencia. Esto mejora el funcionamiento y evita los problemas asociados a un medio de acceso compartido.

Es importante entender qué radio miente en cuál slot. El AP1524SB tiene básicamente 4 slots, pero solamente 3 slots son ocupados por estas 3 radios: AP1524SB: (Slot0) acceso al cliente 2.4GHz; (Slot1 y 2) radios 5GHz: Uplink y regreso del link descendente.

AP1524SB fue iniciado adentro - A, - N y, dominio del C con la versión 6.0.

Nota: En la versión 6.0, las radios 5 gigahertz actúan solamente en la banda 5.8 gigahertz con 5 canales (149 a 165).

Con la versión 7.0, AP1524SB es adentro - E, - dominio disponible K, - M, - S, y T. También, con la versión 7.0, UNII2 y UNII2 más las bandas se han introducido en el dominio A en las radios existentes 5 gigahertz. Como consecuencia, ambas unidades de radio del 802.11a soportan la banda entera 5 gigahertz. Es decir con la versión 7.0 que las radios pueden actúa en UNII-2 (5.25 – 5.35 gigahertz), UNII-2 más (5.47 – 5.725 gigahertz), y las bandas superiores gigahertz del ISMO (5.725 – 5.850).

La Disponibilidad del canal depende del dominio regulador. Total, con la última versión 7.0 usted consigue 5 canales en la banda superior del ISMO, 4 canales en la banda UNII-2, y 11 canales en UNII-2 más la banda. Refiera al cuadro 1 para una descripción general completa de los canales soportados en cada dominio.

Para información de última hora sobre las regulaciones, refiera a las reglas y a las regulaciones de su dominio respectivo del regulador.

Tabla 1: Canales soportados según el dominio regulador

Formación de la malla

Las ubicaciones de la antena para cada radio se reparan y se etiquetan. Ésta es la configuración de las radios con las Antenas:

- Slot0: (11b) (acceso)
- Slot 1: (11a, 5 gigahertz) (acceso universal) – antena direccional Omni/
- Ranura 2: (11a, 5 gigahertz) (regreso) – antena direccional

Una red de interconexión típica

Tal y como se muestra en de esta figura, Slot2 - la radio 5 gigahertz en la punta de acceso a raíz (RAP) se utiliza para ampliar el regreso en la dirección del link descendente, mientras que el slot 2 radio 5 gigahertz en el MAPA se utiliza para el regreso en el uplink. El MAPA extiende la radio del slot1 en la dirección del link descendente. Los faros AWPP se envían solamente en el link descendente para permitir que el niño AP se una a.

Cisco recomienda el usar de una antena direccional con la radio del Slot2 en el mínimo. El razonamiento para esto se explica más adelante en este documento.

La radio del Slot2 (5 gigahertz) internamente está conectada con el puerto de antena 6.

Los puertos de antena se etiquetan como (revestimiento lateral con bisagras adelante):

Puertos de antena en las 1520 Series AP

Los puertos de antena se etiquetan en el hardware y están conectados internamente con las radios en cada slot en el AP1524SB/AP1523CV SKU como:

- Puerto de antena 1: 5 gigahertz (radio del slot1)
- Puerto de antena 2: 2.4 gigahertz (radio del slot0)
- Puerto de antena 3: 2.4 gigahertz (radio del slot0)
- Puerto de antena 4: 2.4 gigahertz (radio del slot0)
- Puerto de antena 5: No conectado
- Puerto de antena 6: 5 gigahertz (radio del Slot2)

Usted tiene que configurar el canal solamente en el RAP para el link descendente, y entonces los mapas harán la selección de canal en una moda automatizada. Los canales se escogen automáticamente del subconjunto del canal, dando cada salto en un diverso canal. Por ejemplo, el canal fijado para la banda 5.8 es {149, 153, 157, 161, 165}. Si el link descendente del RAP se selecciona para ser el canal 153, la selección de canal coge los canales adyacentes alternos para los mapas abajo del árbol de la malla.

Selección de canal en una red de interconexión

Cada salto es no sólo un diverso canal, pero también utiliza diversos pares de radios. Así pues, en términos de slots, éste es cómo parece por el salto:

Slots por el salto en una red de interconexión

Este arreglo no sólo proporciona el alto rendimiento abajo del árbol de la malla, pues la producción no se disminuye exponencial abajo de los saltos con respecto a los modelos AP1522 y AP1524PS, pero también proporciona la alta capacidad y la red robusta contra interferencia.

Nota: Gigahertz de la banda de la seguridad pública (4.94 a 4.99) no se soporta para el regreso o para el acceso al cliente. La razón es que tenemos solamente 2 canales en la lista de la seguridad pública: 20 y 26. La interferencia entre el uplink y el link descendente no se puede evitar usando estos canales. También, la red no puede tener una mezcla de seguridad pública y no de canales de la seguridad pública. Además, usted no puede programar los canales de radio del acceso del regulador para el modelo AP1524SB. Esta asignación es automática dependiendo de la selección de canal para otras radios del slot en el AP.

Aunque sobre todo la radio 2.4 gigahertz sea utilizada por los clientes para acceder la infraestructura de la malla, pero el acceso al cliente está también disponible en dos radios 5 gigahertz. El acceso al cliente en ambas las radios del regreso 5 gigahertz se llama la característica de acceso del Cliente universal. Como el cliente de red inalámbrica de itinerancia puede acercarse al despliegue Lineal AP1524SB de las direcciones encuadernadas del norte y sur, la característica de acceso del Cliente universal en ambas radios 5 gigahertz facilita esto.

Modo de repliegue

Modo de repliegue para un MAPA

El slot1 radio 5 gigahertz en el MAPA también realiza una función más importante. Puede actuar como radio del uplink para el regreso en caso de estos escenarios:

- La radio del Slot2 falla
- La antena para la radio del Slot2 va mala
- La radio del Slot2 no puede encontrar el uplink debido al mún diseño RF
- Interferencia golpea con el pie adentro, y el largo plazo se descolora perturba el uplink a un extender que ranure 2 que la radio suelta la conexión del uplink más a menudo

Cuando la radio del slot1 asume el control para la radio del Slot2, se llama modo de repliegue. La radio del Slot2 se pone para dormir en un canal de la ausencia de interferencias. Es decir el hardware se reduce a AP1522 (dos radios). La radio del slot1 se extiende al uplink. Fijan a un temporizador 15-minute para intentar una pre-exploración para encontrar a un padre en el Slot2 otra vez.

Comportamiento en la selección del padre

Después de que seleccionen a un padre, mantienen y se buscan solamente a los vecinos en el mismo canal que el uplink. La radio del link descendente no buscará para mejores vecinos; será utilizada solamente para extender el árbol para que a los niños entrantes se unan al árbol. La radio del link descendente no procesará ninguna faros que son oída.

Cuando un RAP baja como MAPA (la conexión del RAP al regulador va abajo), utilizará solamente uno de sus radios del regreso para intentar conectar como MAPA (el mejor padre). La segunda radio 5.8 gigahertz no asociará a los clientes y no formará ninguna relación de la malla.

Encaminamiento funcional de tres correspondencias de radio

Para una radio frecuencia Lineal apropiada de la alineación y de la concentración en una dirección, es importante asociar una antena direccional a las radios del Slot2 en el mínimo. Usted debe alinear y ajustar cada link para minimizar el efecto ocultado del nodo. Por ejemplo, en la figura antedicha, el MAPA en la ubicación “C” se debe alinear PARA ASOCIAR en el MAPA de la ubicación “B.” en la ubicación “C” no debe poder ver que el AP en la ubicación “A.” esto puede ser alcanzado primero alineando las Antenas y en seguida optimizando cada link ajustando el poder RF.

Para otros detalles sobre AP1524SB y las características refiera a la versión 7.0 del diseño y del Guía de despliegue de la malla.

Puntos importantes relacionados para enredar la línea de producto

- AP1524SB/AP1523CV puede interoperar completamente con AP1522, AP1524PS, AP1240 y AP1130 como un RAP o MAP.
- Con el código 5.2, el mundo de la malla se combinó detrás con la versión de software principal del regulador, o, es decir introdujimos la malla como única solución con el código 5.2 que está en el cisco.com.
- Muchas nuevas funciones para aumentar la producción y el funcionamiento se han agregado en 6.0 y 7.0 versiones.
- Cisco ha anunciado un fin de la vida útil (EOL) para los mapas AP1505 y AP1510. La fecha más pasada de la venta era de noviembre el 30 de 2008. Animan a los clientes a emigrar sus redes a AP1520s.
- La versión 5.2 o mayor no soporta AP1510 y 1505.

Configuración de la malla

Elija un regulador del Wireless LAN

La solución de la Malla inalámbrica es soportada por las Cisco 2100 Series, el WLCs de las Cisco 4400 Series, el WLCs de las 5500 Series, y el módulo de servicio integrado inalámbrico (WiSM). El Cisco 5500, WiSM, y 4400 reguladores se recomiendan para las implementaciones de la Malla inalámbrica porque pueden escalar a un gran número de AP y pueden soportar la capa 3 CAPWAP.

Nota: Para todas las Plataformas del regulador excepto 5500, los mapas (MALLA los AP) se cuentan como “medios aps.” Es decir malla Aps ()/(de los mapas los rap) se cuentan como “aps llenos” en el regulador 5508.

Como consecuencia, el WiSM modelo de gama alta puede controlar y manejar más de 300 enredan los AP. El WiSM está en el factor de forma de un linecard y cabe en los 6500 y 7600 chasis.

La licencia baja de 5508 reguladores (LIC-CT5508-X) es suficiente para AP al aire libre e interiores (AP152X). La licencia de WPlus (LIC-WPLUS-X) se ha combinado recientemente con la licencia baja y se requiere no más para los mapas interiores (1242s/1130s).

La información detallada sobre los diversos reguladores y sus capacidades se puede encontrar en http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html.

CAPWAP lleva el control y el tráfico de datos entre los AP y el WLC. El tráfico de control es AES-CCM, pero el avión Transport Layer Security (DTL) de los datos no se soporta en la malla.

Después de elegir el regulador, configure el regulador en el modo de la capa 3.

WLC en el modo de la capa 3

Actualice el regulador al código 7.0

Cisco recomienda que usted actualiza el regulador al código 7.0 en el mínimo, pues este código trae en muchas funciones útiles para la movilidad.

Nota: Salve por favor la configuración de controlador corriente con el actual código en un cierto lugar para la referencia antes de actualizar. Si usted tiene que retroceder la red de nuevo al viejo código por cualquier motivo, usted tendrá la configuración práctica. Aunque, la configuración sea preservada durante la actualización al código beta.

Nota: Oficialmente, Cisco no soporta los Downgrades para los reguladores.

De la interfaz GUI del regulador, vaya al **archivo de los comandos** > de la **descarga**. Elija el **código** como el **tipo de archivo** y dé la dirección IP de su servidor TFTP. Defina la trayectoria y el nombre del archivo.

Nota: Utilice por favor al servidor TFTP que soporta más que las transferencias del tamaño del archivo del 32 MB. Por ejemplo, **tftpd32**. Bajo el **trayecto del archivo**, ingrese**./**.

Descarga de imagen en un WLC usando el TFTP

Cuando está acabado de instalar el nuevo firmware, verifique vía el CLI usando el comando del **sysinfo de la demostración** que el nuevo firmware sea de hecho en el lugar:

```
(Cisco Controller) >show sysinfo Manufacturer's Name..............................
Cisco Systems Inc. Product Name..................................... Cisco
Controller Product Version.............................. 6.0.61.0 RTOS
Version..................................... 6.0.61.0 Bootloader
Version.............................. 4.1.171.0 Emergency Image
Version.......................... Error Build Type..................................... DATA +
WPS System Name..................................... SEVT-CONTROLLER System
Location................................. System Contact.................................
System ObjectID................................. 1.3.6.1.4.1.14179.1.1.4.3 IP
Address..................................... 10.51.1.10 System Up
Time................................. 0 days 2 hrs 17 mins 13 secs System Timezone
Location......................... Current Boot License Level....................... Next Boot
License Level.......................... Configured Country.............................. US -
United States Operating Environment........................... Commercial (0 to 40 C) Internal
Temp Alarm Limits...................... 0 to 65 C --More-- or (q)uit Internal
Temperature............................. +53 C State of 802.11b Network.....................
Enabled State of 802.11a Network........................ Enabled Number of
WLANs................................ 1 3rd Party Access Point Support..................
Disabled Number of Active Clients........................ 0 Burned-in MAC
Address............................ 00:0B:85:40:4A:E0 Crypto Accelerator
1............................ Absent Crypto Accelerator 2............................ Absent
Power Supply 1................................. Absent Power Supply
2................................ Present, OK Maximum number of APs
supported.................. 100
```

Agregue los AP

Los mapas pueden unirse a solamente el regulador si la dirección MAC BVI del AP existe en el regulador. La filtración MAC se habilita por abandono. El regulador de Cisco mantiene una lista de la dirección MAC de la autorización del MAPA. El regulador responde solamente a las peticiones de la detección de las radios al aire libre que aparecen en la lista de la autorización. En el regulador, ingrese los direccionamientos MAC de todas las radios que usted utilizará en su red realizando las instrucciones abajo.

Nota: Para AP152X (IOS AP), la dirección MAC BVI se utiliza en el regulador como filtro MAC. Ingrese el MAC address BVI de los AP en el regulador. Para 1240s y 1130s, el MAC Ethernet es el BVI MAC y se debe utilizar en el regulador. Si la dirección MAC del AP no se etiqueta en el AP, publique este comando en la consola AP:

```
At AP console: sh int | i Hardware
```

```
AP0017.94fe.d43f#sh int | i Hardware Hardware is BVI, address is 0017.94fe.d43f (bia
0017.94fe.d43f) Hardware is 802.11G Radio, address is 0017.94fe.d430 (bia 0017.94fe.d430)
Hardware is 802.11A Radio, address is 0017.94fe.d430 (bia 0017.94fe.d430) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba4 (bia 0009.b7ff.dba4) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba5 (bia 0009.b7ff.dba5) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba6 (bia 0009.b7ff.dba6) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba7 (bia 0009.b7ff.dba7)
```

En la interfaz GUI del regulador, vaya a la **Seguridad**, y elija el **MAC que filtra** en el lado izquierdo de la ventana. Haga clic **nuevo…** para ingresar los direccionamientos MAC:

También ingrese los nombres de las radios para la conveniencia bajo **descripción**. Por ejemplo, como los nombres de las calles cruzadas donde las radios han estado instaladas para consulta en cualquier momento.

Seguridad

La otra Seguridad que puede ser conectada es EAP (valor por defecto) o PSK. Usted puede también tomar una decisión del modo seguro como el EAP, el PSK, o autenticación externa en lo mismo página. De la interfaz GUI del regulador, utilice esta trayectoria:

Trayectoria de la interfaz GUI: **Tecnología inalámbrica > malla**.

Seguridad del permiso en un MAPA

La Seguridad se puede también configurar del regulador que usa este CLI:

```
(Cisco Controller) >config mesh security ? eap Enable mesh security EAP for Mesh AP. psk Enable
mesh security PSK for Mesh AP. rad-mac-filter Configure Mesh security radius mac-filter for Mesh
AP. force-ext-auth Configure Mesh security to force external authentication.
```

El modo seguro puede ser verificado en el regulador por estos comandos:

```
(Cisco Controller) >show mesh config Mesh Range..................................... 12000
Backhaul with client access status.............. disabled Background Scanning
State...................... enabled Mesh Security Security
Mode.............................. EAP External-Auth.................................
disabled Use MAC Filter in External AAA server......... disabled Force External
Authentication.................. disabled Mesh Alarm Criteria Max Hop
Count.............................. 4 Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20 Low Link SNR.............................
12 High Link SNR.............................. 60 Max Association
Number...................... 10 Association Interval.......................... 60 minutes
Parent Change Numbers......................... 3 Parent Change Interval.....................
60 minutes --More-- or (q)uit Mesh Multicast Mode............................. In-Out Mesh Full
Sector DFS........................... enabled Mesh Ethernet Bridging VLAN Transparent
Mode..... disabled
(Cisco Controller) >show network summary RF-Network Name............................ SEVT Web
Mode................................... Disable Secure Web Mode.........................
Enable Secure Web Mode Cipher-Option High.......... Disable Secure Web Mode Cipher-Option
SSLv2......... Enable Secure Shell (ssh)......................... Enable
Telnet..................................... Enable Ethernet Multicast Mode...................
Disable Ethernet Broadcast Mode.................... Disable AP Multicast
Mode.......................... Unicast IGMP snooping.............................. Disabled
IGMP timeout................................ 60 seconds User Idle
Timeout........................... 300 seconds ARP Idle Timeout.......................... 300
seconds Cisco AP Default Master..................... Disable AP Join
Priority........................... Disable Mgmt Via Wireless Interface................. Enable
Mgmt Via Dynamic Interface.................. Disable Bridge MAC filter
Config..................... Enable Bridge Security Mode..................... EAP Mesh Full
Sector DFS....................... Enable --More-- or (q)uit Over The Air Provisioning of
AP's........... Disable Apple Talk ............................... Disable AP Fallback
.............................. Enable Web Auth Redirect Ports ................... 80 Fast
SSID Change ......................... Disabled 802.3 Bridging ...........................
Disable
```

La autenticación externa se soporta con el uso de uno o más Ciscos Secure Access Control Server (ACS). El ACS debe ser versión 4.1 o 4.2 corriente.

Nota: El ACS expreso (5.0) no se ha probado explícitamente y las pruebas iniciales indica que es incompatible con los Certificados existentes de VxWorks.

La configuración se requiere en el regulador y el ACS. El soporte para el externo AAA es logrado validando el certificado AP con el certificado instalado en el ACS.

Para una red de interconexión L3, si una está utilizando al servidor DHCP, ponga el regulador en el modo L3. Salve la configuración y reinicie el regulador. Aseegurese le la opción 43 de la configuración en el servidor DHCP. Después de que el regulador haya recomenzado, los AP nuevamente conectados recibirán su dirección IP del servidor DHCP.

La opción 43 se puede utilizar para poblar la tabla de dirección del controlador del RAP con el direccionamiento de un regulador. Esto es muy importante si usted está agregando un RAP a una sección de la red donde debe atravesar un salto de la capa 3 para alcanzar un regulador. Si el RAP nunca ha estado conectado con una subred donde se asocia un regulador, nunca ha podido descubrir esta información.

Los mapas de las Cisco 152X Series validan un formato de la cadena de ASCII para la opción 43 de un servidor DHCP. Las series AP del Cisco Aironet 152X utilizan un formato separado por coma de la cadena para la opción DHCP 43. El otro Cisco Aironet AP utiliza el formato del Type Length Value (TLV) para la opción DHCP 43.

La serie AP152X es una plataforma IOS, así que valida el formato hexadecimal para la opción 43.

Los servidores DHCP deben ser programados volver la opción basada en la cadena del identificador de clase del vendedor del DHCP AP (VCI) (opción DHCP 60).

Para la configuración del Cisco IOS DHCP Server de la opción 43, utilice estos comandos:

```
ip dhcp pool <pool name> network <IP Network> <Netmask> default-router <Default router> dns-server <DNS Server> option 43 hex <0xf1> <1 byte len> <Controller IP addresses>
```

Por ejemplo, si usted quiere configurar 2 IP Addresses de los reguladores para un Huck, usted tiene que configurar la opción 43 como cadena hexadecimal en este formato:

```
option 43 hex f10801041d0301041d21 | ^ ^ ^ | ^ ^ ^1.4.29.33 | ^ ^ | ^ ^1.4.29.3 | ^ | ^ length = 4 * number of ip addresses (4 * 2 = 8) | | f1 is hardcoded value that needs to be added here
```

Aquí está un ejemplo del servidor DHCP (que es un CAT6K que trabaja para el Huck):

```
ip dhcp pool vlan192 network 1.4.29.0 255.255.255.0 default-router 1.4.29.1 option 60 ascii "Cisco AP c1520" option 43 hex f108.0104.1d03.0104.1d21
```

Agregue la opción 60 para AP152X usando este comando:

```
option 60 ascii "Cisco AP c1520"
```

Defina al administrador AP

Para un despliegue L3, usted debe definir al ap-**administrador**. El administrador AP actúa como dirección IP de origen para la comunicación del regulador a los AP.

Ruta: **El regulador > interconecta** > ap-**administrador > edita**.

Administrador AP en el WLC

La interfaz del ap-**administrador** se debe asignar una dirección IP en la misma subred y el VLA N como su interfaz de administración.

Nota: El “AP manager” no se requiere para el WLC 5508. La interfaz de administración sí mismo puede actuar como interfaz dinámica del administrador AP.

Grupo de la movilidad

El grupo de la movilidad permite que los reguladores miren con uno a para soportar la itinerancia inconsútil a través de los límites del regulador. Los AP aprenden los IP de los otros miembros del grupo de la movilidad después de que los CAPWAP se unan al proceso. Un regulador puede ser un miembro de un solo grupo de la movilidad cuyo hasta 24 reguladores son posibles. La movilidad se soporta a través de 72 reguladores. Puede haber hasta 72 miembros (WLCs) en la lista de la movilidad con hasta 24 miembros (WLCs) en el mismo grupo de la movilidad (o el dominio) que participa en la mano-offs del cliente. La ventaja principal de esta característica es que la dirección IP del cliente no tiene que ser renovada en el mismo dominio de la movilidad. Es decir la renovación de una dirección IP es inútil en la arquitectura regulador-basada usando esta característica.

Los clientes pueden vagar por el seamlessly (ninguna renovación de la dirección IP, etc) entre los Grupos de movilidad en un dominio de la movilidad. Un dominio de la movilidad consiste en todos los Grupos de movilidad configurados. El número grande de Grupos de movilidad puede ser creado, constituyendo un dominio de la movilidad. El límite es 72 reguladores suma en un dominio de la movilidad.

Nota: El efectivo del PMK sucede solamente dentro del grupo de la movilidad. Como consecuencia, la itinerancia rápida es posible dentro del grupo de la movilidad, pero la itinerancia inconsútil es posible en un dominio entero de la movilidad (entre los Grupos de movilidad).

Los miembros del regulador de este grupo de la movilidad deben ser presentados manualmente, allí no son ningún protocolo al auto-DISCOVER los otros reguladores que son miembros de nuestro grupo de la movilidad:

Grupo de la movilidad en el WLC

Cuando un cliente de red inalámbrica se asocia y autentica a un AP, el regulador AP pone una entrada para ese cliente en su base de datos del cliente. Esta entrada incluye el MAC y los IP Addresses del cliente, los contextos de seguridad y las asociaciones, los contextos del Calidad de Servicio (QoS), la red inalámbrica (WLAN), y el AP asociado. El regulador utiliza esta información para remitir las tramas y para manejar el tráfico a y desde el cliente de red inalámbrica.

Cuando el cliente de red inalámbrica mueve su asociación a partir de un AP a otro, el regulador pone al día simplemente la base de datos del cliente con el AP nuevamente asociado. En caso necesario, los nuevos contextos de seguridad y asociaciones se establecen también.

Cuando el cliente se asocia a un AP unido a un nuevo regulador, el nuevo regulador intercambia los mensajes de la movilidad por el regulador original, y la entrada de la base de datos del cliente se mueve al nuevo regulador. Los datos son tunneled entre los reguladores que usan el éter en el túnel IP (RFC3378). Los nuevos contextos de seguridad y asociaciones se establecen en caso necesario, y la entrada de la base de datos del cliente es actualizada para el nuevo AP. Este proceso sigue siendo transparente al usuario.

Mensajes de la movilidad en el WLC

Después de la configuración inicial, cada WLC sabrá solamente sobre el regulador local. La información con respecto al otro WLC debe ser introducida. Haga clic en **New**. Usted necesita para cada WLC configurar el otro WLC.

De la interfaz Web, elija el **regulador** > al **grupo de la movilidad**, y agregue el otro WLC con su dirección MAC de la Administración (la dirección MAC se puede encontrar bajo el **regulador** > la

interfaz > Administración) y la dirección IP.

Radie los papeles

Por abandono, un cuadro fresco de los AP tiene un papel de radio de un MAPA. Los mapas tienen una conexión de red inalámbrica y ninguna conexión alámbrica directa al WLC. Los mapas convergen siempre con un RAP.

UN RAP se debe configurar explícitamente como RAP. Esto reduce drástico el esfuerzo de configuración como ahora usted tiene que apenas preconfigurar los rap – y los rap son menos en gran número con respecto a los mapas.

Usted puede utilizar el regulador CLI para preconfigurar los papeles de radio en un AP proporcionó al AP está conectado físicamente con el Switch o usted puede ver el AP en el Switch como un RAP o MAPA:

```
(CiscoController) >config ap role ? rootAP RootAP role for the Cisco Bridge. meshAP MeshAP role for the Cisco Bridge. (CiscoController) >config ap role meshAP ? <Cisco AP> Enter the name of the Cisco AP. (CiscoController) >config ap role meshAP Map3 Changing the AP's role will cause the AP to reboot. Are you sure you want to continue? (y/n) y
```

Papel de un MAPA

Control de la instalación y de la conexión

Despliegue las radios (mapas) en las ubicaciones deseadas.

Refiera al Guía de despliegue para la malla.

Refiera al guía de instalación del hardware.

Conecte el AP que usted quiere como RAP al armario del establecimiento de una red que consiste en el WLC y otros componentes de interconexión de redes, el etc.

Usted debe poder ver todas las radios en el regulador:

Radios en el WLC

```
(Cisco Controller) >show mesh ap summary AP Name AP Model BVI MAC CERT MAC Hop Bridge Group Name
------ ----------------- ---------------- ---------------- --- ----------- HPRAP1 AIR-
LAP1524PS-A-K9 00:1e:14:48:43:00 00:1e:14:48:43:00 0 test HJRAP1 AIR-LAP1522AG-A-K9
00:1d:71:0d:e1:00 00:1d:71:0d:e1:00 0 huckmesh HPMAP1 AIR-LAP1524PS-A-K9 00:1b:d4:a7:78:00
00:1b:d4:a7:78:00 1 test HJMAP1 AIR-LAP1522AG-A-K9 00:1d:71:0c:f4:00 00:1d:71:0c:f4:00 1
huckmesh HJMAP2 AIR-LAP1522AG-A-K9 00:1d:71:0c:f0:00 00:1d:71:0c:f0:00 1 huckmesh HJMAP1 AIR-
LAP1522AG-A-K9 00:1d:71:0d:d5:00 00:1d:71:0d:d5:00 1 huckmesh Number of Mesh
APs..............................  6 Number of RAPs.................................  2 Number
of MAPs.................................  4
```

En la interfaz GUI del regulador, clickWireless ver el RAP y los mapas.

Rap y mapas en el WLC

Si usted tiene más de un regulador conectado con la misma red de interconexión, después usted debe especificar el nombre del controlador primario que usa la configuración global para cada AP, o especifique el controlador primario en cada nodo; si no, el menos regulador cargado será preferido. Si los AP fueron conectados previamente con un regulador, han aprendido ya el nombre del regulador.

Después de que usted configure el nombre del regulador, los AP reiniciarán. Vaya a la pantalla del detalle AP a ver el **controlador primario** AP **nombrar**:

Ruta: **Tecnología inalámbrica > Cisco AP > detalle**.

Controlador primario en el WLC

Aprovéchese de la característica de gran disponibilidad configurando los IP Addresses de los reguladores en cada AP:

Configure la característica de gran disponibilidad en el WLC

Ingresar un IP Address para el controlador de backup es opcional. Si el controlador de backup está fuera del grupo de la movilidad con quien el MAPA está conectado (el controlador primario), después usted necesita proporcionar la dirección IP el primario, secundario, o del controlador terciario, respectivamente. El nombre y la dirección IP del regulador deben pertenecer el mismo primario, secundario, o al controlador terciario. Si no, el MAPA no puede unirse al controlador de backup. La prioridad de la Conmutación por falla AP para los mapas es siempre “crítica.”

Nota: La reinicialización AP después de la Alta disponibilidad se configura.

Detección rogue

Aseegurese que la detección del colorete está apagada para los mapas al aire libre. Se ha inhabilitado por abandono para preservar el ancho de banda del regreso. Sin embargo, es configurable usando este comando:

```
(controller) config mesh ids-state ?
```

permiso - Información de los permisos IDS (detección del granuja/de la firma) para los mapas al aire libre.

neutralización - Información de las neutralizaciones IDS (detección del granuja/de la firma) para los mapas al aire libre.

Nombre de Grupo de Bridge

Los nombres de Grupo de Bridge (BGN) controlan la asociación de los AP. Los BGN pueden agrupar lógicamente las radios para evitar dos redes en el mismo canal de la comunicación con uno a. Esta configuración es también útil si usted tiene más de un RAP en su red en el mismo sector (área). El BGN es una cadena de los caracteres máximo 10.

Un nombre de Grupo de Bridge del fábrica-conjunto se asigna en la etapa de la fabricación (VALOR NULO). No es visible a usted. Como consecuencia, incluso sin un BGN definido, las radios pueden todavía unirse a la red. Las reinicializaciones AP después de la configuración BGN.

Nota: El BGN se debe configurar muy cuidadosamente en una red en funcionamiento. Usted debe salir del nodo más lejano (el nodo más reciente) y moverse siempre hacia el RAP. El razonamiento es que si usted comienza a configurar el BGN en alguna parte en el medio del multihop, después los Nodos más allá de esta punta serán caídos como estos Nodos tendrán un diverso BGN (BGN viejo).

El BGN está vacío por abandono.

Usted puede configurar o verificar el BGN usando el regulador GUI:

Ruta: >All **inalámbrico AP > detalles**.

BGN en el WLC

Si usted tiene una red corriente, tome un AP preconfigurado con un diverso BGN y haga que se une a la red. Usted verá este AP en el regulador que usa el “valor por defecto” BGN después de que usted agregue su dirección MAC en el regulador:

```
(CiscoController) >show mesh path Map3:5f:ff:60 00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT
DEFAULT (106b), snrUp 48, snrDown 48, linkSnr 49 00:0B:85:5F:FA:10 state UPDATED NEIGH PARENT
BEACON (86B), snrUp 72, snrDown 63, linkSnr 57 00:0B:85:5F:FA:10 is RAP
```

Vecinos en el RAP

AP152X usando el valor por defecto BGN como MAPA, asociará a los clientes de red inalámbrica y formará las relaciones de la malla, pero no pasará ningún tráfico del cliente Ethernet.

Aseegurese que usted tiene BGN que corresponden con para cada estímulo del despliegue. También, aseegurese le no tener ningún AP como el “padre predeterminado o niño,” pues estos AP entrarán el modo de exploración después de 15 minutos y la conectividad del cliente será perdida.

El despliegue de la movilidad es muy sensible “omitir los BGN,” pues pierden la Conectividad al nodo primario y a los clientes cada 15 minutos.

Interfaz del regreso

El “regreso” se utiliza para crear solamente la conexión de red inalámbrica entre los AP. La interfaz del regreso por abandono es 802.11a. Usted no puede cambiar la interfaz del regreso a 11b/g.

En AP1524 SB, el Slot2 - la radio 5 gigahertz en el RAP se utiliza para ampliar el regreso en la dirección del link descendente, donde como Slot2 - radio 5 gigahertz en el MAPA se utiliza para el regreso en el uplink. Cisco recomienda el usar de una antena direccional con la radio del Slot2. Los mapas extienden la radio del slot1 en la dirección del link descendente con el Omni o la antena direccional también que proporciona al acceso al cliente. El acceso al cliente se puede proporcionar en la radio del Slot2 a partir del código el 7.0 y posterior.

La velocidad de datos del regreso desempeña un papel importante en un despliegue de la movilidad, pues la velocidad de datos decide al requisito mínimo de la relación señal-ruido (SNR) para cada salto.

Las velocidades de datos también afectan a la cobertura y al rendimiento de la red RF. Las velocidades de datos inferiores (tales como 1 Mbps) pueden extender más lejos del AP que más arriba las velocidades de datos (tales como 54 Mbps). Como consecuencia, la cobertura de célula de las influencias de la velocidad de datos y por lo tanto el número de AP requeridos. Diversas velocidades de datos son alcanzadas enviando una señal más redundante en el link de red inalámbrica, permitiendo que los datos sean recuperados más fácilmente del ruido. El número de símbolos enviados para un paquete a la velocidad de datos del 1 Mbps es mayor que el número de símbolos usados para el mismo paquete en el 11 Mbps. Esto significa que eso el envío de los datos a las velocidades de bits más bajas toma a más tiempo que enviando los datos equivalentes a una velocidad de bits más alta, dando por resultado el rendimiento de procesamiento reducido.

Típicamente, 24 Mb/s se eligen como la tarifa óptima del regreso porque alinea con la cobertura máxima de la porción de la red inalámbrica (WLAN) de la red inalámbrica (WLAN) del cliente del MAPA; es decir, la distancia entre los mapas usando 24 regresos del Mb/s debe permitir la cobertura inconsútil del cliente WLAN entre los mapas. Una velocidad de bits más baja pudo permitir una mayor distancia entre los mapas, pero hay probable ser intervalos en la cobertura del cliente WLAN, y la capacidad de la red de retroceso se reduce. Una velocidad de bits creciente para la red de retroceso cualquiera requiere más mapas o resultados en un SNR reducido entre los mapas, limitando la confiabilidad de la malla y la interconexión.

El comando CLI del regulador para la tarifa del regreso es:

(Regulador de Cisco) > *<ap-name> del rate> del <backhaul del* **bhrate ap de los config**

Adaptación de velocidad dinámica

La adaptación de velocidad dinámica (DRACMA) fue introducida para todas las Plataformas de la malla en la versión 6.0. El Rate Selection es la cosa dominante para la utilización apropiada del espectro disponible RF. Claramente, la tarifa puede también afectar a la producción de los dispositivos del cliente, y la producción es una métrica dominante usada por las publicaciones de la industria para evaluar los dispositivos de los vendedores.

DRACMA introduce un proceso de estimar la velocidad de transmisión óptima para las transmisiones de paquetes. Es importante seleccionar correctamente las tarifas. Si la tarifa es demasiado alta, las transmisiones de paquetes fallarán dando por resultado las fallas en la comunicación. Si la tarifa es demasiado baja, el ancho de banda del canal disponible no será utilizado, dando por resultado los Productos inferiores, y el potencial para el hundimiento catastrófico de la congestión de red.

La velocidad de datos predeterminada para la malla regreso 5 gigahertz sigue siendo 24 MHz. Para aprovecharse de DRACMAS, configure la velocidad de datos del regreso al “auto.” Con la configuración “auto”, enrede el regreso escoge la tarifa más alta donde la tarifa más alta siguiente no puede ser usado debido a las condiciones que no son convenientes para esa tarifa y no debido a las condiciones que afectan a todas las tarifas. Por ejemplo, si el regreso de la malla eligió el 48 Mbps, después esta decisión se ha tomado después de aseegurarse ese nosotros no puede utilizar el 54 Mbps pues no hay bastante SNR para 54 y no porque alguien acaba de girar el horno de microondas que afectará a todas las tarifas.

Para las implementaciones de la movilidad, Cisco recomienda aprovecharse de DRACMAS. AP1524SB provee de usted la mejor producción, y la producción degrada apenas después del primer salto. Su funcionamiento es mucho mejor que AP1522 y AP1524PS, porque estos AP tienen solamente una sola radio para el uplink y el link descendente del regreso.

Con DRACMAS, cada salto utilizará la velocidad de datos mejor para el regreso. La velocidad de datos se puede cambiar sobre una base por-AP.

La velocidad de datos se puede fijar en el regreso sobre una base por-AP. No es comando global. Después de actualizar a 6.0 o de versiones posteriores, el valor preconfigurado de la velocidad de datos del regreso será preservado.

Por ejemplo: Si el Mbps de RAPon =24, MAP1=18 el Mbps etc, entonces las configuraciones son preservados.

Velocidad de datos en el regreso

Utilice este CLI para descubrir a qué tarifa es el regreso:

```
(Cisco Controller) >show ap bhate ? <Cisco AP> Enter the name of the Cisco AP. (Cisco Controller) >show ap bhrate HPRAP1 Backhaul Rate is auto.
```

Utilice este CLI para configurar la tarifa en el regreso:

```
(Cisco Controller) >config ap bhrate ? <rate in kbps> | "auto" Configures Cisco Bridge Backhaul Tx Rate. (Cisco Controller) >config ap bhrate 36000 HPRAP1 (Cisco Controller) >show ap bhrate HPRAP1 Backhaul Rate is 36000.
```

Ahora, si la tarifa se fija al “auto” y usted quiere saber sobre la velocidad actual que es utilizada en el regreso, después utilice este CLI:

```
(Cisco Controller) >show mesh neigh summary HPRAP1 AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- 00:0B:85:5C:B9:20 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:5F:FF:60 0 auto 4 0x10e8fcb8 BEACON DEFAULT 00:0B:85:62:1E:00 165 auto 4 0x10e8fcb8 BEACON OO:0B:85:70:8C:A0 0 auto 1 0x10e8fcb8 BEACON HPMAP1 165 54 40 0x36 CHILD BEACON HJMAP2 0 auto 4 0x10e8fcb8 BEACON
```

En la pantalla antedicha, el RAP está utilizando la velocidad de datos “auto” del regreso, y está utilizando actualmente el 54 Mbps con su MAPA del niño.

Poder y Configuración de canal seriales del MAPA del regreso

Configure el canal solamente en el RAP para el link descendente, y entonces los mapas hacen la selección de canal en una moda automatizada. Los canales se escogen automáticamente del subconjunto del canal que da cada salto en un diverso canal.

Es importante tener presente la estructura del slot para las radios también. Este comando se puede dar para marcar rápidamente el estatus del número de slot de radio:

```
(Cisco Controller 1) >show ap slots Number of APs..... 9 AP Name Slots AP Model Slot0 Slot1 Slot2 Slot3 ----------------- ----- ------------------- ------- ---- ---- ------- ------- HPRAP1 3 AIR-LAP1524PS-A-K9 b/g a-5.8 a-4.9 RAPSB 3 AIR-LAP1524SB-A-K9 b/g a-all a-all HJRAP1 2 AIR-LAP1522AG-A-K9 b/g a-all HPMAP1 3 AIR-LAP1524PS-A-K9 b/g a-5.8 a-4.9 MAP1SB 3 AIR-LAP1524SB-A-K9 b/g a-all a-all HJMAP1 2 AIR-LAP1522AG-A-K9 b/g a-all HJMAP2 2 AIR-LAP1522AG-A-K9 b/g a-all HJMAP3 2 AIR-LAP1522AG-A-K9 b/g a-all MAP2SB 3 AIR-LAP1524SB-A-K9 b/g a-all a-all
```

Del regulador GUI, utilice esta trayectoria: **Tecnología inalámbrica > 802.11a/n** bajo las **radios**.

Estatus del número de slot de radio

Junto con los números de slot de radio respectivos AP ocupados y los papeles de radio se visualizan para un despliegue serial del regreso.

Tal y como se muestra en del tiro de pantalla antedicho, el Slot2 - la radio 5 gigahertz en el RAPSB (regreso serial) se utiliza para ampliar el regreso en la dirección del LINK DESCENDENTE, mientras que slot1 – radio 5 gigahertz en el RAPSB se utiliza para el acceso al cliente. El slot 2 radio 5 gigahertz en el MAPSB se utiliza para el UPLINK, y la radio del slot1 en el MAPSB se utiliza para el Omni o la antena direccional del ACCESO del LINK DESCENDENTE también que proporciona al acceso al cliente, y así sucesivamente. Con la versión 7.0 usted puede también tener acceso al cliente en la radio del Slot2. El tiro de pantalla antedicho se ha tomado con el código 6.0, y se ha cambiado con el código 7.0. Para los detalles, refiérase “se

doblan característica de acceso del Cliente universal 5 gigahertz.

Se dobla el acceso de Cliente universal

Como el cliente de itinerancia puede acercarse la infraestructura de la malla o de la dirección, así que a ella llegan a ser importantes habilitar el acceso al cliente en ambo el regreso las radios 5 gigahertz (slot1 y 2). A partir de la versión de código el 7.0 y posterior, el acceso al cliente es posible en las radios del regreso en AP1524SB y AP1523CV. El acceso al cliente se inhabilita sobre ambas las radios del regreso por abandono.

Aquí están las guías de consulta que se seguirán para habilitar o inhabilitar el acceso al cliente en los números de slot de radio que constituyen las radios 5 gigahertz, con independencia de las radios que son utilizadas como el link descendente o uplink:

- Usted puede habilitar el acceso al cliente en slot-1 incluso si el acceso al cliente en slot-2 se inhabilita.
- Usted puede habilitar el acceso al cliente en slot-1 incluso si el acceso al cliente en slot-2 se inhabilita.
- Si usted inhabilita el acceso al cliente en slot-1 el acceso al cliente en slot-2 se inhabilita automáticamente en el CLI.
- Para solamente inhabilitar el acceso al cliente extendido (en la radio del slot 2) una tiene que utilizar el GUI.
- Todos los mapas reinician siempre que se habilite o se inhabilite el acceso al cliente.

Las dos radios del regreso del 802.11a utilizan la misma dirección MAC. Como consecuencia, puede haber los casos donde los mismos WLAN asocian al mismo BSSID en más de un slot.

Para la documentación purposes, nosotros llamará el acceso al cliente en la radio del Slot2 como acceso universal extendido (EUA).

Configuración

El acceso al cliente sobre ambas las radios del regreso se puede configurar del regulador CLI o del regulador GUI o WCS. Estas configuraciones se explican aquí:

Configuración EUA del regulador CLI

Se utiliza este comando de habilitar el acceso al cliente sobre ambas las radios del regreso. Al ejecutar este comando, un mensaje de advertencia se genera que indica que el “mismo BSSID será utilizado en ambos los slots del regreso y toda la malla serial AP del regreso reiniciará.”

```
config mesh client-access enable extended
```

Se visualiza este mensaje:

```
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh Serial Backhaul APs will be rebooted
Are you sure you want to start? (y/N)
```

El “regreso con el estatus del acceso al cliente” y el “regreso con el estatus ampliado acceso al cliente” se pueden determinar usando el comando del **acceso al cliente de la malla de la demostración**.

show mesh client-access

El estatus aparece:

```
Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): enabled
```

No hay comando explícito de inhabilitar el acceso al cliente solamente en Slot-2 (EUA). Usted tiene que inhabilitar el acceso al cliente en ambos los slots del regreso usando este comando:

config mesh client-access disable

Se visualiza este mensaje:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

Del GUI, usted puede inhabilitar el EUA sin el acceso al cliente que perturba en la radio del slot1. Pero, otra vez, las radios reiniciarán.

Es posible habilitar el acceso al cliente solamente en el slot1 y no en el Slot2 usando este comando:

config mesh client-access enable

Se visualiza este mensaje:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

Configuración EUA del regulador GUI

Del regulador GUI, utilice esta trayectoria: **Tecnología inalámbrica > malla**.

Aquí está una captura de pantalla del regulador GUI cuando se inhabilita el acceso al cliente del regreso:

EUA en el WLC

Elija la casilla de verificación del **acceso al cliente del regreso** para visualizar la casilla de verificación **extendida del acceso al cliente del regreso**. Un mensaje de advertencia será generado después de que usted tecleo **se aplique** con la opción **extendida del acceso al cliente del regreso** marcada:

Acceso al cliente extendido del regreso de la configuración

Una vez que se habilita el EUA, las radios del 802.11a se visualizan como se muestra abajo. El Slot2 - la radio 5 gigahertz en el RAPSB (regreso serial) se utiliza para ampliar el regreso en la dirección del **LINK DESCENDENTE**, y se visualiza como **ACCESO del LINK DESCENDENTE**, mientras que slot1 – radio 5 gigahertz en el RAPSB se utiliza para el acceso al cliente se visualiza como **ACCESO**. Slot2 - la radio 5 gigahertz en el MAPSB se utiliza para el **UPLINK**, se visualiza como **ACCESO del UPLINK** y la radio del slot1 en el MAPSB se utiliza para el **ACCESO del LINK DESCENDENTE** con una antena direccional del Omni también que proporciona al acceso al cliente, y así sucesivamente.

radios del 802.11a

Cree una red inalámbrica (WLAN) en el WLC con el SSID apropiado asociado a la interfaz correcta (VLA N). Cuando usted crea una red inalámbrica (WLAN), consigue aplicada a todas las radios por abandono. Si usted se prepone habilitar el acceso al cliente solamente en la radio del

802.11a, después elija la directiva de radio apropiadamente:

Configure el EUA del WCS

En el WCS, utilice esta trayectoria: **configuración > reguladores > "IP del regulador" > malla > configuraciones de la malla**.

Aquí está la página de la malla WCS cuando se inhabilita el acceso al cliente del regreso:

Elija el **acceso al cliente en el** cuadro de **Verificación del link del regreso** para visualizar la casilla de verificación **extendida del acceso al cliente del regreso**. Un mensaje de advertencia será generado después de que usted haga clic la **salvaguardia** con la opción **extendida del acceso al cliente del regreso** marcada:

Mensaje de advertencia

El canal del regreso no reelige como candidato

El propósito básico de esta característica es proporcionar los medios, usando los cuales el usuario final puede restringir el conjunto de los canales disponibles que se asignará para los rap/los mapas seriales del regreso. Normalmente, para el mundo de la malla, los canales son seleccionados por el usuario para los rap, y el ajuste auto de los mapas PARA GOLPEAR los canales (para AP1522 y AP1522PS) o para seleccionar los canales automáticamente (AP1524SB y AP1523CV). La asignación dinámica del canal (DCA) no fue conectada con el mundo de la malla hasta la versión 6.0. Sin embargo, con la versión 7.0, hay una conexión entre la lista DCA y los mapas del regreso del serial, sólo si alguien utiliza (los permisos) esta característica.

La manera que trabaja es ésa en la eliminación de ciertos canales de la lista DCA, y habilitando el **comando del DCA-canal del regreso de la malla**, esos canales nunca serán asignados a cualquier regreso serial AP, bajo cualquier escenario. Incluso si el radar se detecta en todos los canales dentro de los canales de la lista DCA, la radio será apagada bastante que el movimiento a los canales fuera de ella. Un mensaje trampa será enviado al WCS, y un mensaje será demostración visualizada que la radio se ha apagado debido a los DF. El usuario no podrá asignar el canal al RAP serial del regreso fuera de la lista DCA con el **permiso de los DCA-canales del regreso de la malla de los config**. Sin embargo, éste no es el escenario en el caso de 1522/1524PS AP. Para estos AP, el usuario puede asignar cualquier canal, incluso fuera de la lista DCA en caso del RAP, y el controller/AP puede también seleccionar un canal fuera de la lista DCA en caso de que no hay canal libre del radar disponible desde dentro de la lista.

Puesto que los canales seriales del MAPA del regreso se asignan automáticamente, las ayudas de esta característica en la regulación del conjunto de los canales que consiguen asignaron a los mapas. Por ejemplo, si usted no quiere el canal 165 para conseguir asignado a ningún MAPA 1524, para quitar el canal 165 de la lista DCA y para habilitar esta característica.

Esta característica es más adecuada para los escenarios al aire libre de la interoperabilidad de la malla con los mapas interiores o los WGB que soportan un diferente determinado del canal de los AP al aire libre. Por ejemplo, el canal 165 es soportado por los AP al aire libre pero no por los AP interiores adentro - un dominio.

La característica selecta de la banda facilita la movilidad del WGB o MAR3200 con la infraestructura de la malla, pues permite que el usuario configure un conjunto común de canales disponibles en los mapas y WGB o MAR3200 de itinerancia. Habilitando la característica del deselection del canal del regreso, usted puede restringir la asignación del canal solamente a esos

canales que estén disponibles para los AP autónomos y los AP al aire libre.

Nota: El deselection del canal es solamente posible en el código 7.0 y posterior.

En algunos escenarios, usted puede ser que tenga dos pistas o caminos Lineales para la movilidad de lado a lado. Mientras que sucede la selección de canal de mapas automáticamente, tan puede haber un salto en un canal que no esté disponible en el lado autónomo, o el canal tiene que ser saltado debido lo mismo o al adyacente que es seleccionado en la vecindad AP que pertenece a un diverso encadenamiento Lineal. Usted puede hacer mejores hojas de operación (planning) de la frecuencia en dos estímulos adyacentes haciendo uso de esta característica.

Movilidad de lado a lado

[Configuración del CLI]

1. Utilice el **comando channel avanzado demostración del 802.11a** de revisar la lista del canal configurada ya en la lista DCA:
   ```
   (Controller) >show advanced 802.11a channel Automatic Channel Assignment Channel Assignment
   Mode..... AUTO Channel Update Interval..... 600
   seconds Anchor time (Hour of the day)..... 0 Channel Update
   Contribution..... SNI.. CleanAir Event-driven RRM option.....
   Enabled CleanAir Event-driven RRM sensitivity..... Medium Channel Assignment
   Leader..... 09:2b:16:28:00:03 Last
   Run..... 286 seconds ago DCA Sensitivity
   Level..... MEDIUM (15 dB) DCA 802.11n Channel
   Width..... 20 MHz DCA Minimum Energy Limit..... -95 dBm
   Channel Energy Levels Minimum..... unknown
   Average..... unknown
   Maximum..... unknown Channel Dwell Times
   Minimum..... 0 days, 17 h 02 m 05 s
   Average..... 0 days, 17 h 46 m 07 s
   Maximum..... 0 days, 18 h 28 m 58 s 802.11a 5 GHz Auto-RF
   Channel List Allowed Channel List.....36,40,44,48,52,56,60,64,116,140 Unused
   Channel List.....100,104,108,112,120,124,128,132,136 DCA Outdoor AP
   option..... Disabled
   ```
2. Para agregar un canal a la lista DCA, utilice el **canal avanzado los config del 802.11a agregan el** comando del *number> del <channel*. Usted puede también borrar un número de canal de la lista DCA usando el comando **avanzado los config del** *number> del <channel de la* **cancelación del canal del 802.11a**.**Nota:** Antes de que usted agregue o borre el número de canal de la lista DCA, la red del 802.11a necesita ser inhabilitada. Utilice los **comandos network del permiso del 802.11a de la red** y de los **config de la neutralización del 802.11a de los config** para inhabilitar y habilitar la red del 802.11a respectivamente.También, usted no puede borrar directamente un canal de la lista DCA si se asigna a cualquier RAP serial del regreso. Para borrar un canal asignado a un RAP, usted debe primero cambiar el canal asignado al RAP y en seguida publicar el comando **avanzado los config del** *number> del <channel de la* **cancelación del canal del 802.11a del** regulador.
   ```
   (Controller) >config 802.11a disable network Disabling the 802.11a network may strand mesh
   APs. Are you sure you want to continue? (y/n)y (Controller) >config advanced 802.11a
   channel add 132 802.11a network needs to be disabled (Controller) >config advanced 802.11a
   channel delete 116 802.11a 5 GHz Auto-RF: Allowed Channel List.....
   36,40,44,48,52,56,60,64,116, 132,140 DCA channels for Serial Backhaul Mesh APs is enabled.
   DCA list should have at least 3 non public safety channels supported by Serial Backhaul
   Mesh APs. Otherwise, the Serial Backhaul Mesh APs can get stranded. Are you sure you want
   to continue? (y/N)y Failed to delete channel. Reason: Channel 116 is configured for one of
   the Serial Backhaul RAPs. Disable mesh backhaul dca-channels or configure a different
   channel for Serial Backhaul RAPs. (Controller) >config advanced 802.11a channel delete 132
   802.11a 5 GHz Auto-RF: Allowed Channel List.....
   ```

```
36,40,44,48,52,56,60,64,116, 132,140 DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs. Otherwise, the Serial Backhaul Mesh APs can get stranded. Are you sure you want
to continue? (y/N)y (Controller) >config 802.11a enable network
```

3. Una vez que se ha creado una lista conveniente DCA, utilice el **comando enable de los DCA-canales del regreso de la malla de los config** de habilitar la característica del deselection del canal del regreso para el Punto de acceso serial de la malla del regreso. Usted puede publicar el **comando disable de los DCA-canales del regreso de la malla de los config** en caso de que la característica necesite ser inhabilitada.**Nota:** No se requiere inhabilitar habilitar/neutralización de la red del 802.11a esta característica.

```
(Controller) >config mesh backhaul dca-channels enable 802.11a 5 GHz Auto-RF: Allowed
Channel List..... 36,40,44,48,52,56,60,64,116, 140 Enabling DCA
channels for Serial Backhaul mesh APs will limit the channel set to the DCA channel list.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs. Otherwise, the Serial Backhaul Mesh APs can get stranded. Are you sure you want
to continue? (y/N)y (Controller) >config mesh backhaul dca-channels disable
```

4. Usted puede marcar el estado actual de la característica del deselection del canal del regreso usando el **comando config de la malla de la demostración**.

```
(Cisco Controller) >show mesh config Mesh Range.....
12000 Mesh Statistics update period..... 3 minutes Backhaul with client
access status..... enabled Background Scanning State.....
enabled Backhaul Amsdu State..... disabled Mesh Security Security
Mode..... PSK External-Auth.....
enabled Radius Server 1..... 9.43.0.101 Use MAC Filter in External
AAA server..... disabled Force External Authentication..... disabled Mesh
Alarm Criteria Max Hop Count..... 4 Recommended Max Children
for MAP..... 10 Recommended Max Children for RAP..... 20 Low Link
SNR..... 12 High Link SNR..... 60
Max Association Number..... 10 Association
Interval..... 60 minutes Parent Change
Numbers..... 3 Parent Change Interval..... 60
minutes Mesh Multicast Mode..... In-Out Mesh Full Sector
DFS..... enabled Mesh Ethernet Bridging VLAN Transparent Mode.....
enabled Mesh DCA channels for Serial Backhaul Mesh APs..... disabled
```

5. Para asignar un canal particular a la radio del link descendente de 1524 RAP, utilice el comando del *number> del <channel del <ap-name>* **ap del canal del** *number> del <slot del* **slot de los config**.**Nota:** El Slot2 actúa como radio del link descendente en el caso del RAP 1524SB. También, si se habilita el deselection del canal del regreso, después usted puede asignar solamente esos canales que estén disponibles en la lista DCA.

```
(Cisco Controller) >config slot 2 channel ap RAP2-1524 136 Mesh backhaul dca-channels is
enabled. Choose a channel from the DCA list. (Cisco Controller) >config slot 2 channel ap
RAP2-1524 140
```

Configuración del GUI

Realice estos pasos para configurar la característica del deselection del canal de la lista y del regreso DCA:

Elija el **regulador** > la **Tecnología inalámbrica** > **802.11a/n** > **RRM** > **DCA**, y elija uno o más canales que se incluirán en la lista DCA:

Elija la **Tecnología inalámbrica** > la **malla**, y elija la opción de los **canales de la malla DCA** para habilitar el deselection del canal del regreso usando la lista DCA. Esta opción es aplicable para 1524SB AP.

Realice estos pasos para fijar el canal para la radio del link descendente del RAP:

Elija la **Tecnología inalámbrica** > los **Puntos de acceso** > las **radios** > **802.11a/n**, para configurar los canales en la radio del link descendente del RAP. De la lista de AP, elija la lista desplegable de la antena para un RAP, y elija la **configuración**:

De la sección de la asignación del **canal del regreso RF**, elija la **aduana**, y después elija el canal para la radio del link descendente del RAP:

Información útil/cosas a tener presente

- El canal para la radio serial del acceso del RAP 11a del regreso y ambas radios 11a de los mapas seriales del regreso consiguen asignados automáticamente. No pueden ser configurados por el usuario.
- Mire para el desvío abre una sesión el regulador. En caso de la detección de radar y del cambio subsiguiente del canal, usted verá los mensajes similares a esto:`Channel changed for Base Radio MAC: 00:1e:bd:19:7b:00 on 802.11a radio. Old Channel: 132. New Channel: 116. Why: **Radar**. Energy before/after change: 0/0. Noise before/after change: 0/0. Interference before/after change: 0/0. **Radar signals** have been detected on channel 132 by 802.11a radio with MAC: 00:1e:bd:19:7b:00 and slot 2`
- Para cada regreso serial AP, el canal en su link descendente y radio del uplink debe siempre ser ausencia de interferencias (por ejemplo, si el uplink es el canal 104, ningunos de 100, 104 y 108 canales no se pueden asignar para la radio del link descendente en ese AP). Como consecuencia, el adyacente alterno también se selecciona para la radio del acceso 11a en el RAP.
- En caso de que las señales de radar se detecten en todos los canales excepto el canal de radio del uplink, la radio del link descendente será cerrada y la radio sí mismo del uplink actuará como ambo uplink y link descendente (es decir, el comportamiento es similar a 1522 AP en este caso).
- La detección de radar consigue borrada después de 30 minutos, así que cualquier radio apaga debido a la detección de radar debe ser de reserva y operativa después de esta duración.
- Hay un 60-segundo período del silencio inmediatamente después de la mudanza a un canal habilitado los DF (sin importar si el cambio del canal era debido a la detección de radar o al usuario configurado en caso del RAP), durante el cual el AP se supone analizar para las señales de radar sin transmitir cualquier cosa. Por lo tanto, el pequeño período (60 segundos) de tiempo muerto se puede observar en caso de la detección de radar, si el nuevo canal asignado es también DF habilitados. Si la detección de radar se observa otra vez en el nuevo canal durante el período del silencio, el padre cambiará su canal sin la información del niño AP, pues no se permite transmitir durante el período del silencio. En este caso, el niño AP desasociará y volverá al modo de exploración, redescubre al padre en el nuevo canal, y después se une a detrás, llevando (a un tiempo muerto levemente más largo del minuto aproximadamente tres).
- En el caso del RAP, el canal para la radio del link descendente se selecciona siempre dentro de la lista DCA, sin importar si la característica del deselection del canal del regreso está habilitada o no. El comportamiento es diferente para los mapas, que pueden escoger cualquier canal permitido para ese dominio, a menos que se habilite la característica del deselection del canal del regreso que restringirá el conjunto permitido del canal. Como consecuencia, se recomienda para tener muchos canales agregados a la lista del canal 802.11a DCA para prevenir cualquier radio que consigue debido apagada faltar de los canales incluso si la característica del deselection del canal del regreso es parada.

- Puesto que la misma lista DCA que hasta ahora fue utilizada para RRM la característica también se está utilizando para los mapas a través de la característica del deselection del canal del regreso, tenga presente que cualquier adición/cancelacíon de los canales de la lista DCA afectará a la lista del canal entrada RRM a la característica para no los mapas también. RRM está apagada para la malla.
- **Nota:** En el caso del – El dominio AP M, un intervalo de tiempo levemente más largo se puede requerir para que la red de interconexión suba, puesto que usted ahora tiene una lista más larga de canales habilitados los DF adentro – el dominio M, que cada AP analizará antes de unirse a al padre, y por lo tanto puede tardar a 25%-50% más tiempo que normal unirse a.

Preparación del sitio y hojas de operación (planning)

Cisco recomienda que usted realiza un estudio sobre el sitio de radio antes de instalar el equipo. Un estudio sobre el sitio revela los problemas tales como interferencia, zona de Fresnel, o problemas de la logística. Un estudio sobre el sitio apropiado implica temporalmente el configurar de los links de la malla y el tomar de las medidas para determinar si sus cálculos de la antena son exactos. Esté seguro de determinar la ubicación y la antena correctas antes de los agujeros de perforación, de los cables de la encaminamiento o del equipo del montaje. Visitar cada sitio en donde cada AP tiene que ser ayudas desplegadas mucho. Uno puede ver si hay la línea de visión clara (LOS) disponible en ambas direcciones del norte y sur.

Recomendaciones de instrumentación

Éstas son recomendaciones sobre diseño para los links de la malla:

- El despliegue del MAPA no puede exceder 35 pies en la altura sobre la calle.
- Los mapas se despliegan con las Antenas señaladas en las direcciones del norte y sur con un poco downtilt hacia la tierra para un mejor presupuesto del link y el LOS.
- Las distancias típicas del Rap-a-MAPA 5 gigahertz son 1000 a 4000 pies.
- Las ubicaciones del RAP son típicamente torres, edificios altos, o hilos del cable.
- Las distancias típicas del Mapa-a-MAPA 5 gigahertz son 500 a 1000 pies.
- Las ubicaciones del MAPA son tops típicamente cortos o farolas del edificio. Los mapas no se deben desplegar en los hilos del cable pues no hay módem de cable requerido en los mapas.
- Las 2.4/ distancias típicas del Mapa-a-cliente 5 gigahertz son 300 a 500 pies.
- Las ubicaciones del cliente son típicamente laptopes, CPEs, o Antenas profesionalmente montadas encima del vehículo móvil.

Sea creativo en la selección de las Antenas. Considere siempre el aumento, la directividad, y la polarización junta mientras que elige una antena.

Refiera a antena Aironet de Cisco y al guía de referencia de los accesorios en las antenas de Cisco y los accesorios.

Es recomendable ir con las antenas direccionales bastante que las Antenas omnidireccionales pues la cobertura se enfoca a lo largo de las pistas o de las trayectorias Lineales. Con la colocación apropiada de las antenas direccionales, usted puede centrarse la mayor parte de la energía disponible RF en las pistas. Junto con usar la mayor parte de la energía RF, las antenas direccionales también aumentan el rango.

Las Antenas con una anchura de haz horizontal y vertical de 30-50° son más adecuadas para la

mayor parte de las implementaciones.

Haces

AP1524SB/1523CV tiene 5 N-conectores para asociar 3 2.4 antenas ghz (para la relación de transformación máxima que combina) y el N-conector 2 para 5 antenas ghz. Cada radio tiene por lo menos un puerto del TX/RX. Cada radio debe tener una antena conectada con por lo menos uno de sus puertos disponibles del TX/RX.

Usted puede también elegir las Antenas del no Cisco. Al elegir las Antenas de Cisco exterior, tenga estas cosas presente:

- Cisco no sigue ni mantiene la información sobre la calidad, el funcionamiento, o la confiabilidad de las Antenas y de los cables NON-certificados.
- La Conectividad y la conformidad RF es la responsabilidad del cliente.
- La conformidad se garantiza solamente con las antenas de Cisco o las Antenas que están del mismo diseño y ganan como antenas de Cisco.
- El Centro de Asistencia Técnica de Cisco (TAC) no tiene ningún entrenamiento o historial de cliente con respecto a las Antenas y a los cables del no Cisco.

Aseegurese que usted tiene arreglos apropiados para montar estas antenas remotas al lado de los AP:

En un despliegue satisfactorio típico, el AP1523CVs desplegado cliente en ejecutarse de los hilos del cable paralelo a las vías. Dos antenas direccionales en ambas las radios del regreso fueron utilizadas, como los trenes que llevaban a los clientes de red inalámbrica se acercaban de los ambos lados.

Los soportes de montaje especiales se han iniciado para asociar estas 14 antenas direccionales al AP sí mismo del dBi.

Si el acceso al cliente se requiere en 2.4 gigahertz en el aire libre, después aprovéchese de la relación de transformación máxima que combina usando por lo menos 2 Antenas en AP1520s para la banda 2.4 gigahertz. Hay Antenas compactas disponibles para 2.4 gigahertz que sean convenientes de utilizar.

5GHz radian (802.11a) en las AP1520 Series que el AP es solo adentro destaca la arquitectura (SISO) y la radio 2.4GHz (el 802.11 b/g) es 1x3 solos en arquitectura del múltiplo hacia fuera (SIMO).

La radio 2.4 gigahertz tiene un transmisor y tres receptores. Con sus 3 receptores habilitando la máximo-relación de transformación que combina (MRC), esta radio tiene una mejores sensibilidad y rango que una radio típica SISO 802.11b/g para las tarifas del OFDM. Al actuar con Mb/s más alto de las velocidades de datos de 12, usted puede aumentar el aumento en una radio 2.4-GHz a DB 2.7 agregando dos Antenas y a DB 4.5, agregando tres Antenas.

Hay las 5 antenas ghz de ángulo recto cortas disponibles que se pueden asociar directamente al AP:

Esta captura muestra los mapas desplegados en un top del polo usando 17 Antenas del sector del dBi:

Funcionamiento de pequeñas pérdidas de los cables LMR600 de estas Antenas al MAPA. Aquí, las antenas direccionales se señalan en la dirección opuesta, y están utilizando los canales

adyacentes alternos según el diseño de la red de retroceso serial, así que la separación de la antena está muy bien. Idealmente, usted debe separar las Antenas verticalmente por 10 pies para un plan adyacente alterno. Esto también minimizará la interferencia del “frente” a las radiaciones posteriores del lóbulo.

¿Usted puede preguntarse, donde es el MAPA?

El MAPA está instalado en la tierra. Está conectado con las Antenas en el polo usando los cables de pequeñas pérdidas.

AP instalado en el nivel del suelo

Aseegurese que no hay otros AP de nuestros competidores desplegados al lado de nuestros AP, pues éste puede crear mucha interferencia.

Competidor de cerca desplegado AP

Si hay porciones de árboles con las hojas, pueden absorber la energía RF, y éste puede crear una abolladura grande en el presupuesto del uplink del cliente al AP que se está esforzando ya para una buena conexión RF a la infraestructura de la malla.

Esto llega a ser extremadamente importante asegurarse de que hay “claro” o “cerca” de las condiciones LOS, no sólo entre los AP, pero también entre el tren y el AP.

Si el colgante del AP en los hilos del cable no proporciona las condiciones claras LOS, las medidas especiales del montaje se pueden tomar en los polos de madera como se muestra aquí:

¿También, en relación con el “despliegue Lineal,” qué sucederá si la pista en la cual se está implementando la movilidad da vuelta? El torneado de la pista romperá las conexiones del salto de la malla. Hay maneras de manejar esta situación. Una manera es comienzo al estímulo fresco de los saltos desplegando un RAP en la vuelta. Mucho se requiere instalar un padre AP en estas ubicaciones, pues el link Lineal del salto se romperá si usted no hace además.

RAP instalado en la vuelta

De un ángulo de la logística, busque las Opciones de energía para los AP. Hay las Opciones de energía múltiples que la plataforma AP1520 puede acomodar.

Las Opciones de energía incluyen:

- 90 al poder de la farola de 480 VAC
- 12 V DC
- Poder del cable
- PoE usando un sistema de inyección separado del poderPara los detalles en la inyección del poder, sus especificaciones, y la instalación refieren a las instrucciones de instalación al aire libre del alimentador de corriente del Punto de acceso de la malla del Cisco Aironet de la serie 1520.
- Poder interno del backup de batería
- PoE 802.3af-compliant hacia fuera para conectar los dispositivos IP (tales como cámara de video)

Un módulo opcional del backup de batería (numero de parte AIR-1520-BATT-6AH) está disponible para AP1520s. La batería integrada se puede utilizar para el poder de reserva temporal durante las interrupciones de la alimentación externa. El tiempo de ejecución de la batería para AP1520s es:

- APoperation de tres horas usando 2 radios en 77°F (25°C) con el puerto de egreso del PoE apagado.
- operación de dos horas AP usando dos radios en 77°F (25°C) con el puerto de egreso del PoE encendido.

Nota: La batería no se soporta en la configuración del cable AP.

- Para marcar rápidamente, si los AP están llevando la batería, y si las baterías están cargadas o no, utilice este comando que también muestre el estatus de los cuatro uplinks, del calentador, y de la temperatura de cada AP. Este comando se puede también funcionar con en a por la base AP:

```
(Cisco Controller) >show mesh env summary AP Name Temperature(C/F) Heater Ethernet Battery -
---------------- ---------------- ------ -------- ------- HPRAP1 38/100 OFF UpDnNANA N/A
HPRAP1 33/91 OFF DnDnNANA N/A HJRAP1 39/102 OFF UpDnNANA 94 % HJMAP3 33/91 OFF DnDnNANA 95 %
HJMAP2 35/95 OFF DnDnNANA 99 % HJMAP1 35/95 OFF DnDnNANA 94 % AP1510Map 33/91 OFF DOWN N/A
```

Ratios señal/ruidos

Al hacer la célula que planea y que decide a las distancias entre los AP, es importante decidir a las cosas como el espaciamiento típico entre los AP, el conteo saltos, el SNR mínimo entre los AP (Nodos) etc.

Cisco recomienda que la distancia máxima entre los dos nodos adyacentes no debe exceder 2000 pies. La distancia típica es 1000 pies. Los saltos máximos en una dirección de un RAP deben ser guardados a cuatro saltos para un mejor control de las cosas.

Esta tabla muestra el SNR mínimo del link para cada velocidad de datos del regreso:

Tabla 2: Velocidades de datos del regreso y requisitos mínimos de LinkSNR

Velocidad de datos	SNR requerido mínimo del link
54 Mbps	DB 31
48 Mbps	DB 29
36 Mbps	DB 26
24 Mbps	DB 22
18 Mbps	DB 18
12Mbps	DB 16
9 Mbps	DB 15
6 Mbps	14 dB

El valor mínimo requerido de LinkSNR es conducido por la velocidad de datos y esta fórmula:

SNR + margen de desvanecimiento mínimos

- El SNR mínimo refiere a un estado ideal de la ausencia de interferencias, del NON-ruido, y de un índice de errores del paquete del sistema (POR) de no más el que 10%.
- La margen de desvanecimiento típica es aproximadamente DB 9 a 10.
- No recomendamos el usar de mayor de 24 Mb/s de las velocidades de datos en las implementaciones municipales de la malla pues los requisitos del SNR no hacen las distancias prácticas. Es el mejor utilizar la característica dinámica de la asignación de la tarifa

para que la tarifa del regreso ajuste como los requisitos disponibles del SNR.

Para una radio frecuencia Lineal apropiada de la alineación y de la concentración en una dirección, es importante asociar una antena direccional a las radios del Slot2 en el mínimo. Usted debe alinear y ajustar cada link para minimizar el efecto ocultado del nodo. Los nodos secundarios deben considerar y seleccionar solamente al padre inmediato, bastante que saltando encima al salto siguiente y seleccionando el AP respectivo como padre. Esto puede ser alcanzada primero alineando las Antenas y en seguida optimizando cada link ajustando el poder RF.

Hay algunos comandos útiles que deben ser utilizados para marcar la salud de los links entre los Nodos.

muestre que la malla y la malla de los config son comandos potentes usados para verificar la interconexión en su red:

(Cisco Controller 1) >show mesh ? env Show mesh environment. backhaul Show mesh AP backhaul info. neigh Show AP neigh list. path Show AP path. astools show mesh astools list stats Show AP stats. secbh-stats Show Mesh AP secondary backhaul stats. per-stats Show AP Neighbor Packet Error Rate stats. queue-stats Show AP local queue stats. security-stats Show AP security stats. ap Show mesh ap summary config Show mesh configurations. secondary-backhaul Show mesh secondary-backhaul ids-state Show mesh ids-state client-access Show mesh backhaul with client access. public-safety Show mesh public safety. cac Show mesh cac.
(Cisco Controller 1) >config mesh ? linktest Run linktest on the backhaul between two neighboring APs. linkdata Retrieves sampled link test data from a AP. range range from RAP to MAP Cisco Bridge (150..132000) astools Configures mesh anti-stranding. public-safety Enable/Disable 4.9GHz Public Safety Bands for Mesh AP. battery-state Disables the Battery-State for an AP client-access Enable/Disable backhaul with client access CiscoAP. multicast Configure Mesh Multicast Mode. security Set Bridge Security Mode. radius-server Configure Mesh Radius Server full-sector-dfs Configure Mesh full sector DFS status. ids-state Configures enabling/disabling of IDS)Rogue/Signature Detection) Reporting for Outdoor Mesh APs alarm Configure mesh alarm parameters. backhaul Config Mesh Backhaul. ethernet-bridging Mesh

El comando path de la malla de la demostración mostrará las direcciones MAC, el papeles de radio de los Nodos, el canal, y el SNR del link en el DB para un trayecto determinado:

(Cisco Controller) >show mesh path HPRAP1 AP Name/Radio Channel Rate Link-Snr Flags State ---------- ----------- ------- ---- -------- ------- ----- HPRAP1 is a Root HP. (Cisco Controller) >show mesh path HPMAP1 AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- HPRAP1 165 auto 37 0x10e8fcb8 UPDATED NEIGH PARENT BEACON HPRAP1 is a Root AP.

El canal mostrado en el comando antedicho corresponde al canal de radio del Slot2 en caso del despliegue serial del regreso usando AP24SB/1523CV.

El comando del relincho de la malla de la demostración muestra las direcciones MAC, las relaciones controlante/subordinado, link SNRs en el DB:

(Cisco Controller) >show mesh neigh ? detail Show Link rate neigh detail. summary Show Link rate neigh summary. (Cisco Controller) >show mesh neigh summary HJRAP1 AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- 00:0B:85:5C:B9:20 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:5F:FF:60 0 auto 3 0x10e8fcb8 BEACON 00:0B:85:62:1E:00 165 auto 2 0x10e8fcb8 BEACON 00:19:30:76:32:72 0 auto 4 0x10e8fcb8 BEACON 00:1B:0C:DE:13:34 0 auto 4 0x10e8fcb8 BEACON HJMAP2 161 54 45 0x36 CHILD BEACON HJMAP1 161 54 65 0x36 CHILD BEACON HJMAP3 161 54 44 0x36 CHILD BEACON **(Cisco Controller) >show mesh neigh summary HJMAP1** AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- 00:0B:85:5C:B9:20 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:5F:FF:60 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:62:1E:00 165 auto 17 0x10e8fcb8 NEEDUPDATE BEACON DEFAULT 00:19:30:76:32:72 0 auto 19 0x10e8fcb8 BEACON 00:1B:0C:DE:13:34 0 auto 5 0x10e8fcb8 BEACON 00:1B:54:D1:FA:CE 0 auto 0

```
0x10e8fcb8 BEACON HJMAP2 161 auto 37 0x10e8fcb8 UPDATED NEIGH BEACON HJMAP3 161 auto 38
0x10e8fcb8 NEIGH BEACON HJMAP1 161 36 59 0x24 UPDATED NEIGH PARENT BEACON
```

El comando del **árbol ap de la malla de la demostración** visualiza el conteo saltos, el SNR del link, y el BGN:

```
(Cisco Controller) >show mesh ap tree ================================================== ||
AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
================================================== [Sector 1] ---------- RAP[0, 0, shobhit]
|-MAP1[1, 26, shobhit] |-MAP2[2, 14, shobhit] ----------------------------------------------
-- Number of Mesh APs.............................. 3 Number of
RAPs.................................. 1 Number of MAPs................................. 2 --
----------------------------------------------
```

Infraestructura de itinerancia del cliente usando el modo WGB

Un WGB es una pequeña unidad autónoma que puede proporcionar una conexión de infraestructura de red inalámbrica para los dispositivos activados por Ethernet. Los dispositivos que no tienen un adaptador de red inalámbrica de cliente para conectar con la red inalámbrica se pueden conectar con el WGB a través del acceso de Ethernet.

Un WGB es un dispositivo que los socios a un AP y proporcionan Puente transparente a sus clientes atados con alambre. Cada cliente atado con alambre que el WGB aprende en su interfaz Fast Ethernet consigue señalado a la raíz WGB por el uso de la Mensajería de la punta del Inter-acceso (IAPP). El IAPP es propietario de Cisco; trabaja solamente con Cisco AP.

El WGB también proporciona un uplink fuerte hacia la infraestructura AP usando su potencia alta y ganancia de antena. El cliente convencional integrado en la laptop no puede proporcionar este tipo de uplink fuerte pues ha limitado el poder y casi 0 ganancias de antena del dBi.

Itinerancia en el modo WGB

Para la infraestructura de itinerancia, usted puede o utilizar la tecnología inalámbrica de Cisco AP autónomos en el modo WGB o el indicador luminoso LED amarillo de la placa muestra gravedad menor WMIC en MAR3200 se puede configurar como WGB para la conexión de Wifi a la infraestructura AP instalada a lo largo de las pistas ferroviarias, del camino, o del túnel.

Se configura con el **Workgroup Bridge del papel de la estación**.

Hay otro modo inalámbrico similar llamado Universal WGB (uWGB). Esta configuración permite que el WGB se asocie a la red de infraestructura de Wifi como cliente, él se llama “universal” porque se ve del AP como cliente normal con una sola dirección MAC (la dirección MAC de MARC). El WGB universal fue hecho para tener el WGB/WMIC compatible con el no Cisco AP. No se ata al IAPP o a CCX.

Se configura con el **MAC address universal del Workgroup Bridge del papel de la estación**, el MAC address que es el que está visto infra del AP.

el uWGB no es tan flexible como el WGB en el sentido que solamente un solos cliente/interfaz puede ser soportado detrás de él. Hay pocas ventajas del uWGB, como él es puede ser poco más rápido como ningún IAPP, es NON-CCX, y puede hablar con cualquier infraestructura AP (no Cisco incluyendo). Sin embargo, el WGB puede soportar MAC/clients múltiple detrás de él sin tuvo que NAT o ruta.

Nota: Interoperabilidad al aire libre del modo del uWGB del soporte de los mapas. También, el

uWGB se soporta solamente en MAR3200 802.11bg WMIC 3201. No se soporta en WMICs 3202 (4.9 gigahertz) y 3205 (5 gigahertz).

Hay dos modos en WGB AP autónomos: Modo del modo de infraestructura y del cliente BSS. El modo de infraestructura soporta los VLAN múltiples detrás del WGB, y el modo del cliente BSS soporta solamente solo un VLA N detrás del WGB.

Con el código 6.0 en la arquitectura unificada corriente, Cisco soporta la asociación WGB a un LWAPP/CAPWAP AP solamente en el modo del cliente (o BSS). No hay soporte del modo de infraestructura como en el caso de solución autónoma. Como consecuencia, el WGB es tratado como cliente de red inalámbrica normal por el regulador. Es decir Cisco no soporta los VLAN múltiples detrás del WGB.

Con el código 7.0, los VLAN múltiples detrás del WGB se soportan para los clientes atados con alambre solamente. Esto proporciona la segregación del tráfico basada en los VLA N para diversas aplicaciones que se ejecutan en diversos dispositivos conectados con un Switch detrás de un WGB en la red de interconexión. Si un cliente tiene una red de interconexión que consiste en típicamente 1524 AP con el regreso dual, el tráfico de los clientes WGB será enviado en el priority queue derecho en el regreso de la malla basado en los valores DSCP/dot1p.

Nota: Usted necesita una imagen autónoma especial en los AP autónomos que son utilizados como el WGB o MARCHA para la Interoperabilidad con la infraestructura unificada CAPWAP.

Recomendamos el elegir de ninguno de estos AP que se utilizarán como WGB: AP1240, AP1250, AP1130, AP1310, o MAR3200.

Los AP con las antenas externas, como el AP1240, deben ser dados la preferencia mientras que dan un presupuesto del link comparativamente mejor.

El WGB es completamente interoperable con la infraestructura al aire libre e interior de la malla.

Interoperabilidad WGB

- BH — Regreso
- RAP/MAP — Muestra los AP específicos que son utilizados como combinaciones RAP/MAP.

Nota: La característica de acceso del Cliente universal no está disponible en un modelo AP1524PS (seguridad pública).

Nota: Aunque estemos diciendo aquí que usted puede utilizar el AP1250 AP como WGB, debe ser claro que usted no puede salir las ventajas 802.11N de él, como usar las secuencias múltiples, velocidades de datos más altas y la vinculación del canal, etc. Esto es una limitación porque estas características no están disponibles en el lado de la infraestructura de la malla todavía, aunque los mapas utilicen las técnicas SISO y SIMO. 5GHz radian (802.11a) en las AP1520 Series que el AP es arquitectura SISO y la radio 2.4GHz (el 802.11 b/g) es arquitectura 1x3 SIMO.

Una radio 2.4 gigahertz tiene 1 transmisor y 3 receptores. Con sus 3 receptores habilitando la máximo-relación de transformación que combina (MRC), esta radio tiene una mejores sensibilidad y rango que una radio típica SISO 802.11b/g para las tarifas del OFDM.

Por ejemplo, usted no configura el canal en el WGB, pues es un cliente. Usted configura el canal en el AP. Como consecuencia, si el AP se configura con un canal ancho 40MHz, después el WGB debe ser capaz de usar las tarifas superiores MCS. Sin embargo, configurar canales más anchos

que 20 MHz no es posible en el lado de la malla todavía. Además, Cisco tiene solamente 1 esquema del transmisor (1x3), así que la herencia 802.11a/b/g solamente es posible.

Por otra parte, Cisco no ve ninguna ventajas de usar un AP1252 contra 1242 como WGB en una red debido 11g/11a a estas razones:

- Cuesta más.
- Es mucho más grande y más pesado.
- Utiliza más poder.
- No soporta el valor de la “distancia” (no relevante enredar, sería relevante para un cliente WGB de un Bridge IOS).

Las ventajas de los 1252 (un CPU más rápido, más DRAM y flash, carruaje contra 100baseT) - ninguno de él proporcionarían cualquier ventaja práctica en una aplicación 11g/a.

Scalability de itinerancia

Cisco unificó la arquitectura proporciona mucho scalability. Según lo descrito anterior, el WLCs puede acomodar el número grande de AP. Usted puede agregar fácilmente los reguladores para la Redundancia. Hasta 72 reguladores pueden ser parte de al cluster N+1. Un dominio de la movilidad (que consiste en varios Grupos de movilidad) es un número que consiste en de la área de cobertura de AP agrupados juntos en cuál un cliente puede hacer que seemless vague por sin perder su sesión. La determinación de itinerancia del scalability debe comenzar con una idea de cuántos AP pueden estar en un solo dominio de la movilidad.

Si usted considera un ejemplo de WiSM, un solo regulador de WiSM puede manejar hasta 300 AP. Es posible tener tres Grupos de movilidad. Cada grupo de la movilidad puede tener hasta 24 reguladores. Por lo tanto, es posible tener 7200 AP en un solo grupo de la movilidad. Esta manera, la solución puede escalar más de 100 millas. Como un cliente puede también ayunar libremente vague por dentro de los Grupos de movilidad y el diseño se puede escalar hasta 72 reguladores con el seamlessly de itinerancia del cliente (itinerancia no rápida pues el PMK no se cobra entre los Grupos de movilidad). Así pues, usted puede tener hasta 21600 AP que prueban la itinerancia inconsútil para muchas millas.

Semejantemente, si usted considera el WLC 5508, puede manejar hasta 500 AP. Así pues, para 72 reguladores para que un cliente vague por el seamlessly usando 3 Grupos de movilidad, usted puede tener 36000 AP, provding otra vez la itinerancia inconsútil para las millas.

En el lado de la Administración, 1 WCS puede manejar hasta 3000 AP, o hasta 750 reguladores en la mayor capacidad. En la de menor capacidad, 500 AP y 50 reguladores. El navegador WCS puede manejar 20 WCS y 20,000 AP.

Soporte del cliente de red inalámbrica en el WGB

Los AP con dos radios como WGB proporcionan ciertamente una mejor ventaja, pues una de las radios se puede utilizar para el acceso al cliente y la segunda radio se puede utilizar para acceder los AP. Tener 2 radios independientes que hacen 2 funciones independientes proporciona un mejor control y baja el tiempo de espera. También, los clientes de red inalámbrica en la segunda radio para el WGB no consiguen desasociados por el WGB sobre perder su uplink o en un escenario de itinerancia. En términos más simples, una radio tiene que ser configurada como raíz (papel de radio) y la segunda radio tiene que ser configurada como WGB (papel de radio).

Nota: Si una radio se configura como WGB, después la segunda radio no puede ser un WGB o un repetidor.

Estas características no se soportan para el uso con un WGB:

- El híbrido COSECHA
- Tiempo de inactividad
- Autenticación Web: Si un WGB se asocia a una red inalámbrica (WLAN) de la autenticación Web, el WGB se agrega a la lista de la exclusión, y borran a todos los clientes atados con alambre WGB. (la red inalámbrica (WLAN) de la autenticación Web es otro nombre para la red inalámbrica (WLAN) del invitado.)
- Para los clientes atados con alambre detrás de la filtración WGB, MAC, de las pruebas del link, y del tiempo de inactividad.

Puntas a recordar antes de configurar

- Cisco recomienda el usar de la radio 5 gigahertz para que el uplink ASOCIE la infraestructura. De esta manera, usted puede aprovecharse del acceso al cliente fuerte en dos radios 5 gigahertz disponibles en los mapas. También, la banda 5 gigahertz permite sobre todo más Effective Isotropic Radiated Power (EIRP), y se contamina menos. En dos WGB de radio, configure la radio 5 gigahertz (modo de la radio 1) como WGB. Esta radio será utilizada para acceder la infraestructura de la malla. Configure la segunda radio modo 2.4 gigahertz (radio 0) como raíz para el acceso al cliente.
- En los AP autónomos, solamente un SSID se puede asignar al VLAN nativo. Los VLAN múltiples en un SSID no son posibles en el lado autónomo. Es decir la asignación del SSID-a-VLA N debe ser única, como ésta es la manera que segregamos el tráfico en diversos VLA N. Por otra parte, en una arquitectura unificada, los VLAN múltiples se pueden asignar a una red inalámbrica (WLAN) (SSID).
- Solamente una red inalámbrica (WLAN) (SSID) para la asociación de red inalámbrica del WGB a la infraestructura AP se soporta. Este SSID se debe configurar como infraestructura SSID y se debe asociar al VLAN nativo. El WGB caerá todo que no está en el VLAN nativo hacia la infraestructura de la malla.
- La interfaz dinámica se debe crear en el regulador para cada VLA N configurado en el WGB.
- La segunda radio (2.4 gigahertz) en el AP se debe configurar para el acceso al cliente. Usted tiene que utilizar el mismo SSID en las radios y la correspondencia al VLAN nativo. Si usted crea un SSID separado, después usted no podrá asociarlo al VLAN nativo, debido a los requisitos únicos de la asignación VLAN/SSID. Y, si usted intenta asociar el SSID a otro VLA N, después usted no tiene soporte del VLAN múltiple para los clientes de red inalámbrica según hoy.
- Soportan a todos los tipos de la Seguridad L2 para los WLAN (SSID) para la asociación del cliente de red inalámbrica en el WGB.
- Esta característica no tiene ninguna formalidad en la plataforma AP. En el lado del regulador, se soportan la malla y la NON-malla AP.
- Hay una limitación de 20 clientes en el WGB, si el WGB está hablando con la infraestructura AP basada en la arquitectura unificada. Esos 20 clientes incluyen atado con alambre y los clientes de red inalámbrica. Si el WGB está hablando con los AP autónomos, después el límite del cliente es muy alto.
- El regulador trata la Tecnología inalámbrica y a los clientes atados con alambre detrás del

WGB como lo mismo, así que las características como la prueba el macfiltering y del link no se soportan para los clientes inalámbricos WGB del regulador.
- Si procede, un usuario puede funcionar con una prueba del link para el cliente de red inalámbrica WGB de un AP autónomo.
- Los VLAN múltiples para los clientes de red inalámbrica asociados al WGB no se soportan.
- Los VLAN múltiples hasta 16 se soportan para los clientes atados con alambre detrás del WGB de la versión 7.0 y posterior.
- La itinerancia se soporta para la Tecnología inalámbrica y los clientes atados con alambre detrás del WGB. El WGB sobre perder su uplink o en un escenario de itinerancia no disociarán a los clientes de red inalámbrica en la otra radio.

Cisco le recomienda la radio 0 (2.4 gigahertz) de la configuración como raíz (una del modo de operaciones para el AP autónomo) y radia 1 (5 gigahertz) como WGB.

Ejemplo de configuración

Éstos son obligatorios cuando usted configura del CLI:

1. dot11 SSID (la Seguridad para la red inalámbrica (WLAN) se puede decidir sobre la base del requisito).
2. Asocie las interfaces sub en ambas las radios a un grupo de un solo Bridge.**Nota:** El VLAN nativo se asocia siempre al Grupo de Bridge 1 por abandono. Para el otro número VLAN de las coincidencias del número de Grupo de Bridge de los VLA N, como para el VLA N 46, el Grupo de Bridge es 46.
3. Asocie el SSID a las interfaces radio y defina el papel de las interfaces radio.

En este ejemplo, un SSID (WGBTEST) se está utilizando en las radios y el SSID es la infraestructura SSID asociada al VLAN NATIVO 51. Todas las interfaces radio se asocian al Grupo de Bridge -1.

```
WGB1#config t WGB1(config)#interface Dot11Radio1.51 WGB1(config-subif)#encapsulation dot1q 51
native WGB1(config-subif)#bridge-group 1 WGB1(config-subif)#exit WGB1(config)#interface
Dot11Radio0.51 WGB1(config-subif)#encapsulation dot1q 51 native WGB1(config-subif)#bridge-group
1 WGB1(config-subif)#exit WGB1(config)#dot11 ssid WGBTEST WGB1(config-ssid)#vlan 51 WGB1(config-
ssid)#authentication open WGB1(config-ssid)#infrastructiure-ssid WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1 WGB1(config-if)#ssid WGBTEST WGB1(config-if)#station-role
workgroup-bridge WGB1(config-if)#exit WGB1(config)#interface Dot11Radio0 WGB1(config-if)#ssid
WGBTEST WGB1(config-if)#station-role root WGB1(config-if)#exit
```

Usted puede también utilizar el GUI de un AP autónomo para configurar estas cosas. Del GUI, las subinterfaces se crean automáticamente una vez que se define el VLA N.

Control de la asociación WGB

La asociación WGB a la asociación del regulador y del cliente de red inalámbrica al WGB se puede verificar usando el **comando client de las asociaciones del dot11 de la demostración** en el AP autónomo:

```
WGB#show dot11 associatoions client 802.11 Client Stations on Dot11Radio1: SSID [WGBTEST] : MAC
Address IP address Device Name Parent State 0024.130f.920e 10.51.1.10 LWAPP-Parent RAPSB - Assoc
```

Del regulador, elija el **monitor** > a los **clientes**. El WGB y la Tecnología inalámbrica/el cliente atado con alambre detrás del WGB serán actualizados y muestran la Tecnología inalámbrica/el cliente atado con alambre como el cliente WGB:

Resultado de la prueba del link

Una prueba del link se puede también funcionar con del regulador CLI usando este comando:

(Cisco Controller) > linktest *<client mac address>*

La prueba del link del regulador se limita solamente al WGB, y no puede ser ejecutada más allá del WGB del regulador a atado con alambre o cliente de red inalámbrica conectado con el WGB. Usted puede funcionar con la prueba del link para el cliente de red inalámbrica conectado con el WGB del WGB sí mismo usando este comando:

ap#dot11 dot11Radio 0 linktest target <client mac> Start linktest to 0040.96b8.d462, 100 512 byte packets ap# POOR (4 % lost) Time Strength(dBm) SNR Quality Retries msec In Out In Out In Out Sent : 100,Avg 22 - 37 - 83 48 3 Tot: 34 35 Lost to Tgt: 4, Max 112 - 34 - 78 61 10 Max: 10 5 Lost to Src: 4, Min 0 - 40 - 87 15 3 Rates (Src/Tgt) 24Mb 0/5 36Mb 25/0 48Mb 73/0 54Mb 2/91 Linktest Done in 24.464 msec

WGB atado con alambre/cliente de red inalámbrica

Los comandos de TheseCLI son también convenientes de utilizar:

(Cisco Controller) >show wgb summary Number of WGBs..... 2 MAC Address IP Address AP Name Status WLAN Auth Protocol Clients ----------------- --------------- ---------------- --------- ---- ---- --- 00:1d:70:97:bd:e8 9.47.184.54 c1240 Assoc 2 Yes 802.11a 2 00:1e:be:27:5f:e2 9.47.184.55 c1240 Assoc 2 Yes 802.11a 5 **(Cisco Controller) >show client summary** Number of Clients..... 7 MAC Address AP Name Status WLAN/Guest-Lan Auth Protocol Port Wired 00:00:24:ca:a9:b4 R14 Associated 1 Yes N/A 29 No 00:24:c4:a0:61:3a R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:61:f4 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:61:f8 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:0a R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:42 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:71:d2 R14 Associated 1 Yes 802.11a 29 No **(Cisco Controller) >show wgb detail 00:1e:be:27:5f:e2** Number of wired client(s): 5 MAC Address IP Address AP Name Mobility WLAN Auth ----------------- --------------- ----------------- ---------- ---- ---- 00:16:c7:5d:b4:8f Unknown c1240 Local 2 No 00:21:91:f8:e9:ae 9.47.184.83 c1240 Local 2 Yes 00:21:55:04:07:b5 9.47.184.66 c1240 Local 2 Yes 00:1e:58:31:c7:4a 9.47.185.75 c1240 Local 2 Yes 00:23:04:9a:0b:12 Unknown c1240 Local 2 No

WGB que vaga por

El tiempo de itinerancia es el tiempo llevado por el papel de la radio WGB para desasociar a partir de un AP y para reasociar a otro AP. Durante este intervalo, no hay Transferencia de datos, y, por lo tanto, el tiempo de itinerancia es significativo mantener las sesiones.

Observe por favor que el papel WGB se puede fijar en cualquier AP autónomo o en los indicadores luminosos LED amarillo de la placa muestra gravedad menor uces de los mic de la Tecnología inalámbrica (WMIC) del MARCHA (MAR3200).

La itinerancia implica dos procesos principales:

- El analizar
- Reasociación

El analizar

El WGB soporta a dos modos principales de vagar por la operación:

- Modo “estático” del valor por defecto - La itinerancia se basa en dos variables principales: retransmisiones de paquete, o pérdida de ocho faros consecutivos.
- Modo móvil de la estación - Encima de las variables anteriores, el AP puede hacer el análisis periódico de los descensos del nivel de la señal y de las rotaciones de la velocidad de datos.

Básicamente, hay cuatro condiciones que accionan el WGB para comenzar a analizar para un mejor AP:

- La pérdida de ocho faros consecutivos.
- Una rotación en la velocidad de datos.
- Se excede la cuenta de reintentos máxima de los datos (el valor predeterminado es 64).
- Un período de tiempo medido de un descenso en el umbral de la potencia de la señal.

Solamente los dos elementos más recientes de esta lista son configurables y se explican aquí. El resto se cifra difícilmente. Cuando es un de los sobre los criterios se encuentra, WGB accionará un proceso de itinerancia, analizando aproximadamente 10 a 20ms/channel. Usted puede también limitar los canales que se analizarán con la configuración. El uso recomendado de los canales en el despliegue es 3 para 802.11b/g en caso de aplicación del rendimiento alto, aunque para los escenarios bajos del flujo de datos, él es posible utilizar un conjunto reducido, para minimizar el tiempo de la exploración.

Analizar la metodología seguida es “exploración activa.” En vez de escuchar los faros de los AP, el WGB enviará activamente la “petición de la sonda: ” paquetes y esperas para que 20ms consiga una respuesta en cada canal. El AP parará el analizar después de que reciba la primera respuesta con una señal satisfactoria. Así pues, el período de la exploración puede durar aproximadamente 40ms. Esta vez puede ser más corta dependiendo del tipo de hardware de radio.

Workgroup Bridge de la configuración para vagar por

Hay dos formularios principales para configurar los parámetros de itinerancia WGB:

- Utilice las recomprobaciones del paquete.
- Utilice el **comando station móvil**.

Las recomprobaciones del paquete permiten un más enfoque conservador, donde el WGB no comenzará un proceso de itinerancia, hasta que se detecte la pérdida de datos o se faltan ocho faros consecutivos.

La estación móvil comenzará un proceso regular en el WGB para hacer la itinerancia “con derecho preferente”, que monitorea los niveles de la señal y los cambios de velocidad de la tarifa, y fuerza una nueva itinerancia antes de que la señal actual AP sea demasiado baja. Este proceso de la exploración accionará los pequeños intervalos en la transmisión de radio cuando la radio está realizando la exploración del canal.

Los comandos both toman esta forma, bajo interfaz dot11Radio:

```
ap(config-if)#packet retries <data retry count> {drop} ap(config-if)#mobile station period X threshold Y (in dBm)
```

Si el WGB comienza a analizar debido a una pérdida de ocho faros consecutivos, el mensaje “demasiados faros faltados” se visualiza en la consola. En este caso, el WGB está actuando como cliente universal del Bridge, como cualquier otro cliente de red inalámbrica en su comportamiento.

En algunas situaciones, es interesante utilizar la opción opcional del “descenso” en las

recomprobaciones del paquete, para preservar la asociación, incluso en el error transmitir un paquete de datos. Esto es útil para desafiar los entornos RF, donde la itinerancia se puede también accionar por el comando de exploración móvil.

El algoritmo móvil de la estación evalúa dos variables: la rotación y la potencia de la señal de la velocidad de datos y responde como:

- Si el driver hace un largo plazo abajo desplace en la tarifa del transmitir para los paquetes al padre, el WGB inicia una exploración para un nuevo padre (no más que una vez cada periodo configurado).
- Si el driver hace un largo plazo abajo desplace en la tarifa del transmitir para los paquetes al padre, el WGB inicia una exploración para un nuevo padre (no más que una vez cada periodo configurado).

La rotación de la data rate se puede visualizar usando este comando:

```
debug dot11 dot11Radio 0 trace print rates
```

Sin embargo, esto no mostrará el algoritmo de la rotación de la tarifa de datos reales en la acción, sino solamente los cambios en la velocidad de datos. Esto determina el período de tiempo para explorar, dependiendo de cuánto fue disminuida la velocidad de datos.

El período móvil de la estación se debe fijar dependiendo de la aplicación. El valor predeterminado es 20 segundos. Este período de retraso evita que el WGB analice constantemente para un mejor padre si, por ejemplo, el umbral está debajo del valor configurado.

Algunas situaciones pueden requerir un temporizador más rápido; por ejemplo, en los trenes de alta velocidad. El período no debe ser más bajo que el tiempo que es requerido por el AP para completar el proceso de autenticación. Por ejemplo, para el 802.1x + las redes del CCKM, no debe ser fijado debajo de 2 segundos. Las redes del PSK pueden utilizar al segundo. El período real tendrá siempre el segundo agregado al temporizador, producto de la resolución del planificador de trabajos AP para esta tarea.

Las configuraciones del umbral el nivel en el cual el algoritmo se acciona para analizar para un mejor padre. Este umbral se debe fijar a noise+20dBm pero no más que -70dBm (+70 porque está entrado para el umbral es positivo). El valor por defecto es el dBm -70. El umbral correcto dependerá de la velocidad de datos prevista, contra el nivel de la cobertura ofrecido en el entorno donde el WGB actuará. Si se asume que una cobertura apropiada, debemos fijar este umbral para ser un poco menos que punto entonces el “de desempate” para la velocidad de datos necesaria para las aplicaciones funcionando.

Cuando usted habilita estas configuraciones, el WGB analiza para una nueva asociación de padre cuando encuentra un indicador pobre de la fuerza de señal recibida (RSSI), interferencia de radio excesiva, o un alto porcentaje de la pérdida de trama. Usando este los criterios, un WGB configurado como estación móvil buscan para una nueva asociación de padre y vagan por a un nuevo padre antes de que pierda su asociación actual. Cuando se inhabilita la configuración móvil de la estación (la configuración predeterminada) el WGB no busca para una nueva asociación hasta que pierda su asociación actual.

Los valores de umbral se deben fijar según la banda de frecuencia usada, pues se relaciona directamente con la interferencia. Por ejemplo, el umbral para 2.4 gigahertz se debe fijar un poco más alto (por DB 5) con respecto a 5GHz o a la banda 4.9 gigahertz pues la banda 2.4 gigahertz tiene comparativamente más interferencia. Observe por favor que el umbral tiene valores

negativos.

Por ejemplo:

- Para 2.4 gigahertz`ap(config-if)#mobile station period 3 threshold 70`
- Para 5 gigahertz`ap(config-if)#mobile station period 3 threshold 75`

Configure un Workgroup Bridge para la exploración limitada del canal

En los entornos móviles tales como ferrocarriles, un WGB en vez de analizar todos los canales será restringido para analizar solamente un conjunto de los canales limitados para reducir el retardo de la mano-apagado cuando el WGB vaga por a partir de un AP a otro. Limitando el número de canales el WGB analiza solamente a ésos requeridos, el WGB móvil alcanza y mantiene una conexión continua de la red inalámbrica (WLAN) con rápido y el roaming ininterrumpido. Este conjunto limitado del canal se configura usando este comando CLI:

`ap(config-if)#mobile station scan <set of channels>`
El comando CLI invoca la exploración a todos o a los canales especificados. No hay limitación en el número máximo de canales que puedan ser configurados. El número máximo de canales que puedan ser configurados es restringido solamente por el número de canales que una radio puede soportar. Cuando está ejecutado, el WGB analiza solamente este conjunto limitado del canal. Esta característica limitada del canal también afecta a la lista sabida del canal que el WGB recibe del AP al cual se asocia actualmente. Los canales se agregan a la lista sabida del canal solamente si son también una parte del conjunto limitado del canal.

Aquí está un ejemplo de configuración para las configuraciones de itinerancia ya mencionadas:

```
ap(config)#interface dot11radio 1 ap(config-if)#ssid outside ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge ap(config-if)#mobile station ap(config-if)#mobile
station period 3 threshold 50 ap(config-if)#mobile station scan 5745 5765
```
No utilice el **ningún** comando de **exploración móvil de la estación** de restablecer la exploración a todos los canales.

Las correspondencias leveraged las mejoras del 802.11 WNBU para la itinerancia rápida, tal como QBSS IE, información vecina AP, Cisco centralizó la administración de claves (CCKM), las correspondencias etc. implementa las mejoras CCXV4 como el AP ayudado vaga por, lista vecina aumentada, y vaga por el informe de la razón. El tiempo de itinerancia también depende de las configuraciones de la seguridad de red inalámbrica (autenticación y cifrado) del WGB y de la red inalámbrica (WLAN) que son utilizados.

Está siendo consciente del tiempo largo de la exploración que avanza el tiempo de espera de la entrega más arriba, tres tipos de exploraciones implementadas para el WGB:

- Exploración normal
- Ayuna la exploración
- Exploración muy rápida

Una exploración normal comienza por el canal asociado y continúa completando un ciclo con el resto de los canales. Por ejemplo, si el WGB con 13 canales fue asociado a un AP en el canal 6, el WGB comenzará su exploración en el canal 6 entonces 7, 8, 9, 10, 11, 12, 13, 1, el 2,3, 4 y 5. sobre analizar los 11 canales y recibiendo más de una respuesta de la sonda, el WGB realizará una función del comparar que compare todos los AP de respuesta al que fue asociado previamente en a los medios del nivel de la señal, de la carga, y de los saltos. Si había solamente

un solo AP de respuesta, el WGB no realizará la función y los intentos del comparar para autenticar y para asociarse inmediatamente al nuevo AP.

El WGB realiza una **exploración rápida** cuando el tráfico está entre 10 y 20 paquetes por segundo. El WGB analiza y se asocia al primer AP de respuesta durante una exploración rápida.

Durante una **exploración muy rápida**, el WGB no analiza en absoluto e intenta asociarse al mejor AP de la lista adyacente que se aumenta con el IAPP y CCX.

Después de que se complete cualquier procedimiento de la exploración, el WGB compara los AP de respuesta e intenta autenticar y asociarse al mejor AP.

El WGB compara los AP de respuesta

Soporte de la lista del vecino de la configuración

Según lo mencionado previamente, el WGB recibirá una lista vecina del otro padre potencial AP que están en el área. En algunos escenarios, es interesante quitar esto, pues la lista de padre puede tener “direccionalidad.” Por ejemplo, en un túnel, como el tren está moviendo encendido una dirección dada, la lista recibida es solamente parcialmente válido, como algunos de los vecinos para el padre actual AP no serán accesibles en la dirección que el tren está moviendo (el tren se está moviendo lejos de algunos de ellos).

```
ap(config-if)# mobile station ignore neighbor-list
```

Reasociación

Una vez que encuentran a un vecino AP que satisface las características de señal, el WGB iniciará conmutar encima al AP siguiente. El WGB realizará estos pasos:

1. Pare el transmitir hasta que finalicen los datos.
2. Envíe el pedido de autenticación.
3. Reciba la respuesta de autenticación.
4. Envíe la petición de la reasociación.
5. Reciba la respuesta de la reasociación.
6. Haga la autenticación del 802.1x.
7. Haga el intercambio de EAPoL.
8. Comience a transmitir los datos sobre el nuevo AP.

Ejemplos estándar del proceso de asociación del 802.11

Para todos los temporizadores mencionados aquí, no consideramos las retransmisiones o los descansos que pueden variar de sistema a sistema debido a la configuración o a la implementación (la infraestructura autónoma y unificada tiene diversos valores de agotamiento del tiempo por ejemplo). Las retransmisiones del Protocolo de Autenticación Extensible (EAP) pueden extenderse de 100ms a varios segundos de largo, y las retransmisiones del radio están normalmente en el área de 2 a 5 segundos. Mostramos aquí un escenario del “mejor caso”, con poco o nada de suceso de las retransmisiones. En la vida real, es posible que algunas retransmisiones están observadas, dependiendo de la calidad y/o de la utilización de la red RF.

La actualización IAPP es un conjunto del intercambio de paquetes entre el WGB y el WLC/WDS. Este intercambio puede llevar alrededor 10 200ms. Esto se necesita solamente en el modo WGB. Si usa al modo WGB universal, este paso no está ocurriendo. Permite que el WGB informe los dispositivos detrás de él, y comienza su flujo de tráfico.

El paso 1 consiste en el AP que agota su cola actual de la radio TX. Puede tardar pocos milisegundos dependiendo de cómo está ocupado está el media RF, y de cuántos paquetes se hacen cola en la radio en el momento que la itinerancia está accionada. Pues esto no es fiable, no lo agregue al cálculo. Esto puede tomar un máximo de 4 segundos en el peor de los casos.

Los pasos 2-3 intercambios de paquetes son manejados directamente por el AP raíz, y pueden suceder en 1-2ms típicamente.

Los pasos 4 y 5 se envían al WLC en la infraestructura unificada, y se deben dirigir en otro 2ms más cualquier retraso de propagación agregado por la red entre el AP y el WLC. En el caso de una infraestructura autónoma (IOS), son manejados directamente por el AP.

Setp 6: el 802.1x proporciona los WLAN con fuerte, la autenticación recíproca entre un cliente y un servidor de autenticación. Además, el 802.1x proporciona dinámico por usuario, las claves de encripción del por session, quitando la carga administrativa y los problemas de seguridad que rodean las claves de encripción estáticas. el 802.1x es soportado por el modo de la WPA-empresa y el modo WPA2-Enterprise.

Con el 802.1x las credenciales usadas para la autenticación, tal como contraseñas del inicio, nunca se transmiten en el claro, o sin el cifrado, sobre el media inalámbrico. Mientras que la autenticación del 802.1x proporciona la autenticación robusta para la Tecnología inalámbrica LAN vía un método EAP. El TKIP o el AES también se necesita para el cifrado además del 802.1x puesto que la encripción WEP estándar del 802.11 es vulnerable a los ataques a la red.

Después de que la autenticación recíproca se haya completado con éxito, el cliente y el servidor de RADIUS cada uno derivan la misma clave de encripción, que se utiliza para cifrar todos los datos intercambiados. Usando un canal seguro en el LAN cableado, el servidor de RADIUS envía la clave al regulador del Wireless LAN, que la salva para el cliente. El resultado está por usuario, las claves de encripción del por session, con la longitud de una sesión determinada por una directiva definida en el servidor de RADIUS. Cuando expira una sesión o el cliente vaga por a partir de un AP a otro, un reauthentication ocurre y genera una nueva clave de la sesión.

Algunos tipos EAP son más seguros que otros – es decir EAP-LEAP tiene el nombre de usuario/la contraseña como un mschap tiene pero es frágil, EAP-MD5 y EAP-NULL son muy inseguros.

Éstos son tan más seguro que el nombre de usuario/la contraseña es con los túneles seguros del tipo:

- EAP-FAST (autenticación adaptable de EAP vía el Tunelización seguro)
- EAP-TLS (Transport Layer Security)
- PEAP (protocolo extensible authentication protegido)
- EAP-TTLS (TLS EAP-tunneled)

Cisco no recomienda el uso del SALTO debido a las vulnerabilidades conocidas con los establecimientos de diccionario. EAP-rápidos o EAP-TLS son los métodos de autenticación más seguros recomendados.

De la lista arriba, solamente el EAP-FAST y el EAP-TLS se soportan en el WGB. El EAP-TLS requiere a un servidor de certificados.

El EAP-TLS es más seguro en el hecho que con el EAP-FAST el usuario/la contraseña puede ser copiado, con el EAP-TLS, nosotros utiliza un certificado que trabaje solamente en el hardware específico.

El EAP-TLS fue desarrollado por la Microsoft Corporation para habilitar el uso del EAP como extensión del PPP de proporcionar la autenticación dentro del PPP y del TLS para proporcionar integridad-protegió la negociación y el intercambio de claves de la habitación de la cifra.

El EAP-TLS, que se define en el RFC 2716, utiliza el control de acceso certificado-autenticado Public Key Infrastructure (PKI) del acceso basado del IEEE 802.1X X.509 y se apunta específicamente para dirigir varias debilidades en otros protocolos EAP tales como EAP-MD5. Sin embargo, en la dirección de estas debilidades, la complejidad de los aumentos del despliegue debido al hecho de que no sólo los servidores, pero también los clientes requieren los Certificados para la autenticación recíproca.

El EAP-FAST fue desarrollado por Cisco y sometido al IETF como Borradores de Internet en febrero 2004. Los Borradores de Internet fueron revisados y sometieron en abril 2005. El protocolo del EAP-FAST es una arquitectura de seguridad del servidor del cliente que cifra las transacciones EAP dentro de un túnel de TLS. Mientras que es similar al PEAP a este respecto, diferencia perceptiblemente en que basan al establecimiento del túnel del EAP-FAST sobre las claves secretas compartidas fuertes que son únicas a los usuarios. Estos secretos se llaman las credenciales protegidas del acceso (PAC) y se pueden distribuir automáticamente (aprovisionamiento automático o de la en-banda) o manualmente (aprovisionamiento manual o fuera de banda) a los dispositivos del cliente. Porque los apretones de manos basados sobre los secretos compartidos son intrínseco más rápidos que los apretones de manos basados sobre una infraestructura PKI, el EAP-FAST es el perceptiblemente más rápido que el EAP-TLS que proporciona las transacciones cifradas EAP. El EAP-FAST puede utilizar los Certificados para autenticar su fase 2 usando el EAP-TLS dentro del túnel interno.

la autenticación del 802.1x puede variar de 20ms a varios segundos. La razón es los intercambios adicionales de la trama entre el cliente y el servidor del authenticator del final más eso cualquier temporizador de retransmisión en el EAP que puede tardar uno o más segundos. Esto puede implicar el hablar con un servidor de RADIUS y/o una Base de datos de usuarios externa, que pueden agregar un cierto retardo en el proceso.

el 802.1x utiliza un método EAP para la autenticación, cada tipo puede necesitar una diversa cantidad de intercambios completar. Por ejemplo, el SALTO puede acabar en apenas 2 tramas, pero es unsecure. El EAP-TLS puede necesitar 10 o más intercambios dependiendo del tamaño del certificado.

Paso 7: Después de que se complete el 802.1x el dispositivo necesita completar el intercambio de EAPoL para acabar la generación del material clave para comenzar el cifrado de los datos del usuario. Ésta es 4 tramas, y puede tomar alrededor de 20ms para acabar

Paso 8: Después de que se complete la autenticación y se negocia el material clave, el cifrado puede comenzar, y el WGB ahora ahora envía los datos sobre el nuevo AP.

Cisco centralizó la administración de claves (el CCKM)

Para minimizar el tiempo de la autenticación del 802.1x, Cisco soporta el “rápido asegura” la característica de itinerancia (del CCKM). Con la característica del CCKM, el 802.1x puede suceder adentro alrededor de 50-100ms.

Cada vez que el WGB reasocia con un nuevo AP, necesita reautentificar. Dependiendo del tipo de autenticación, esto puede aumentar el tiempo de itinerancia especialmente en que un servidor de AAA está implicado.

Como se muestra aquí con el SALTO, seis intercambios son necesarios con el servidor de RADIUS completar la autenticación. (el EAP es similar):

Ejemplo del SALTO

El CCKM utiliza una técnica de reintroducción rápida que permita a los clientes para vagar por a partir de un AP a otro. La autenticación completa 802.1x/EAP no se requiere. El CCKM reduce el tiempo requerido por el cliente para autenticar mutuamente con el nuevo AP y para derivar una nueva clave de la sesión durante la reasociación. La itinerancia segura rápida del CCKM se asegura de que no hay retardo perceptible en las aplicaciones sensibles al tiempo. El CCKM es una característica CCXv4-compliant.

Ejemplo del CCKM

Con el CCKM, la primera asociación del WMIC a la infraestructura hará una autenticación completa del 802.1x + la negociación del material clave que toman las medidas según lo descrito previamente.

Entonces en los eventos de itinerancia siguientes, el CCKM hará la autenticación al mismo tiempo que hace la reasociación (pasos 4 y 5), y entonces la reutilización del material clave previamente negociado, en la primera asociación.

El CCKM quitará generalmente el 802.1x y los tiempos de EAPoL del proceso de itinerancia completo.

La itinerancia de alta velocidad del Cisco Compatible Extension (CX), los clientes de la versión 4 (v4) se soporta en acelera a 70 mph en las implementaciones al aire libre de la malla de AP1522s y de AP1524s. El tiempo de itinerancia depende de las diversas cosas, y esto se ha explicado más adelante en esta sección.

Se soportan 3 mejoras de itinerancia del cliente de la capa 2 de Cisco CX v4:

- **Itinerancia ayudada Punto de acceso** — Esta característica ayuda a los clientes salva el tiempo de la exploración. Cuando un cliente de Cisco CXv4 se asocia a un AP, envía un paquete de información al nuevo Punto de acceso que enumera las características de su AP anterior. El tiempo de itinerancia disminuye cuando el cliente reconoce y utiliza una lista del Punto de acceso construida compilando todos los AP anteriores a los cuales cada cliente era asociado y enviado (unicast) al cliente inmediatamente después de la asociación. La lista AP contiene los canales, BSSIDs del vecino AP que soportan el SSID actual del cliente, y el tiempo transcurrió desde la desasociación.
- **Lista vecina aumentada** — Esta característica se centra en la mejora de un cliente de Cisco CX v4 vaga por el funcionamiento de la experiencia y del borde de la red, especialmente al mantener las Aplicaciones de voz. El AP proporciona su información del cliente asociada sobre sus vecinos que usan un mensaje del unicast de la actualización de la vecino-lista.
- **Vague por el informe de la razón** — Esta característica permite a los clientes de Cisco CX v4 para señalar la razón por la que vagaron por a un nuevo AP. También permite que los administradores de la red construyan y que monitoreen un historial de la itinerancia.

Cifrado

La red del Cisco Unified Wireless incluye el soporte para las certificaciones WPA y WPA2 del Wi-Fi Alliance. El WPA fue introducido por el Wi-Fi Alliance en 2003. El WPA2 fue introducido por el

Wi-Fi Alliance en 2004. Todo el con certificación Wi-Fi de los Productos para el WPA2 se requiere ser interoperable con los Productos que son con certificación Wi-Fi para el WPA.

El WPA y el WPA2 ofrecen un nivel elevado de garantía para los usuarios finales y los administradores de la red que sus datos seguirán siendo soldado y que el acceso a sus redes será restringido a los usuarios autorizados. Ambos tienen modos de operación personales y de la empresa que cubran las necesidades distintas de los dos segmentos de mercado. El modo de empresa de cada uno utiliza el IEEE 802.1X y el EAP para la autenticación. El modo personal de cada uno utiliza el PSK para la autenticación. Cisco no recomienda al modo personal para las implementaciones del negocio o del gobierno porque utiliza un PSK para la autenticación de usuario. El PSK no es scalable y seguro para los entornos para empresas. El WPA dirige todas las vulnerabilidades sabidas WEP en la instrumentación de seguridad original del IEEE 802.11 que trae una solución acerca de la seguridad inmediata a los WLAN en la empresa y los entornos del small office/home office (SOHO). El WPA utiliza el TKIP para el cifrado. El WPA2 es la última generación de Seguridad del Wi-Fi. Es la implementación interoperable de Alliance del Wi-Fi del estándar ratificado de IEEE 802.11i. Implementa el algoritmo de encripción AES recomendado del National Institute of Standards and Technology (NIST) usando el modo contrario con el protocolo del Message Authentication Code del Cipher Block Chaining (CCMP). El WPA2 facilita la conformidad del gobierno FIP 140-2.

Para la red inalámbrica (WLAN) en el WLC, utilice WPA1 o el WPA2. Para el WPA2, el **AES** se marca por abandono, y para WPA1, el **TKIP** se marca por abandono:

Nota: Los WGB no pueden asociarse a los mapas si la red inalámbrica (WLAN) colligated se configura con WPA1 (TKIP), +WPA2 (AES), y la interfaz WGB correspondiente se configura con SOLAMENTE una de estos cifrados (WPA1 o WPA2).

WPA(2)-PSK

En este mecanismo, el PSK se utiliza para crear directamente en parejas la clave principal (PMK) que desvía el proceso del 802.1x. Todavía tiene que hacer un intercambio de EAPoL.

El tiempo de itinerancia real (exploración + reasociación + por encima):

Tiempo de itinerancia de la aplicación = tiempo de la exploración + tiempo de la reasociación + overheads WLC/WDS (actualización IAPP).

Para WPA(2)-PSK las sincronizaciones son 20-40ms (exploración de itinerancia) + 2ms (pedido de autenticación) + 2ms (req del assoc) + 20ms (EAPoL) + 3-100ms (IAPP). **Pudo variar a partir del ms el 47 – 164.**

autenticación del 802.1x (sin el CCKM)

Para las sincronizaciones are20-40ms (exploración de itinerancia) de la autenticación del 802.1x + 2ms (pedido de autenticación) + 2ms (req del assoc) + 20-2500ms o más (dot1x) + 20ms (EAPoL) + 3-100ms (IAPP). **Pudo variar a partir del ms el 67 – 2664.**

autenticación del 802.1x más el CCKM

20-40ms (exploración de itinerancia) + 2ms (pedido de autenticación) + 2ms (req del assoc) + 3-100ms (IAPP). **Pudo variar a partir del ms el 27 – 144.**

Conclusión

El CCKM es menos susceptible a los problemas, pues tiene solamente dos tramas que necesiten ser enviadas correctamente para completar el cambio de estado de itinerancia. El tiempo total para acertado vaga por está en la media muy pequeña, que es útil para la Voz y/o los aplicación de video.

El PSK es una alternativa, pero en la media cada hora de itinerancia es más lenta que el CCKM y más probable fallar debido a los problemas RF (más intercambios de paquetes necesarios). También, es puede ser menos segura dependiendo de la clave de autenticación usada. La ventaja es un tiempo de recuperación más rápido, en comparación con el 802.1x lleno necesario en el escenario de falla del CCKM.

La diferencia principal en el PSK contra el CCKM, es ésa para el PSK, cualquier retransmisión del proceso de EAPoL multiplicará el tiempo total. En el PSK usted necesita completar seis intercambios de las tramas (asociación + EAPoL M1 a M4), que son la mayoría del punto crítico, pues cualquier error aquí afectará al tiempo de itinerancia total.

UN CCKM que vaga por el error significa que la itinerancia siguiente es 802.1x basado (lento), después los roamings subsiguientes son CCKM otra vez.

La situación es simple: cualquiera utilizan el almacenamiento en memoria inmediata dominante, que soportamos y recomendamos para ser CCKM, o trabajan en una itinerancia basada 802.1x, con las épocas entre 1 y 20 segundos en cada uno vagando por, que no es fiable.

Tabla 3: Números de rendimiento de itinerancia y otros

Tipo de la Seguridad	Retardo de itinerancia	Probabilidad
802.1x WPA2 con el CCKM	< 200 milisegundos	el 95% de tiempo
802.1x WPA2 con el CCKM	200 milisegundos – 800 milisegundos	el 4% de tiempo
802.1x WPA2 con el CCKM	> 800 milisegundos	el 1% de tiempo

Nota: Las tecnologías de red inalámbrica se diseñan usando los sistemas de radio que están conforme a interferencia de la onda de radio. Las causas de esta interferencia pueden ser accidentales o deliberadas. Sin importar la fuente, interferencia puede interrumpir la conexión de red inalámbrica, inhabilitando cualquier solución que dependa del WI-FI. Dado tales riesgos, las soluciones que afectan la seguridad pública no deben depender SOLAMENTE de las tecnologías de red inalámbrica. Redundante, se prefieren el solapar, y los sistemas independientes (e.g atado con alambre y Tecnología inalámbrica). En el contexto de los sistemas de control del tren, los ejemplos de solapar, los sistemas redundantes incluyen pero no se limitan a: emparejar las tecnologías de red inalámbrica con dos o más sistemas independientes, sistemas mecánicos (e.g. “Switch del deadman "), señalización de control del tren sobre los carriles metálicos, y descuido humano a bordo y central (driver del tren) o supervisores del control central. Si un sistema fallara, otro sistema independiente todavía estaría disponible, ayudando reduce los riesgos a la seguridad pública.

Consejos de Troubleshooting

Si un cliente de red inalámbrica no se está asociando a un WGB, realice estos pasos para resolver problemas:

1. Verifique la configuración del cliente y aseegurese la configuración del cliente es apropiado.
2. Marque la salida del **Bridge de la demostración** en el AP autónomo y conforme el AP está leyendo el MAC Address del cliente en la interfaz correcta.
3. Confirme que las interfaces del submarino correspondiente a los VLAN determinados en diversas interfaces están asociadas al mismo Grupo de Bridge.
4. Si procede, borre la entrada del Bridge usando el **comando clear bridge** (recuerde este comando quitará a toda la haber atado con alambre y clientes de red inalámbrica asociados en el WGB y hará que se asocian otra vez).
5. Marque la salida de la **asociación del dot11 de la demostración** y conforme WGB se asocia al regulador con éxito.
6. El WGB tiene una limitación 20-client, así que aseegurese le no haber excedido el límite.

En las circunstancias normales si el **Bridge de la demostración** y las salidas de la **asociación del dot11 de la demostración** están como se esperaba, la asociación del cliente de red inalámbrica debe ser acertada.

Si hay algunos problemas del uplink WGB, estos comandos pueden ser utilizados:

```
debug dot11 d0/1 tr pr uplink debug dot11 wpa-cckm-km-dot1x debug dot11 mgmt msg debug dot11 mgmt int
```

Escenarios importantes

- Los clientes de red inalámbrica deben ser tratados como un cliente normal para un AP autónomo y características como el ACL, el MAC que filtra, y la autenticación de los LR que pueden ser aplicables para estos clientes si están configurados del WGB (se soportan todas las características autónomas).
- Los clientes de red inalámbrica en la otra radio no deben ser disociados por el WGB sobre perder su uplink o en un escenario de itinerancia.
- El Multicast se debe soportar para los clientes de red inalámbrica detrás del WGB.
- Los clientes de red inalámbrica detrás del WGB deben conseguir el mismo privilegio de un cliente atado con alambre detrás del WGB en el regulador.

VLAN múltiples y soporte de QoS para los clientes atados con alambre WGB

Descripción general de características

Un WGB es una pequeña unidad autónoma que puede proporcionar una conexión de infraestructura de red inalámbrica para los dispositivos activados por Ethernet. Los dispositivos que no tienen un adaptador de red inalámbrica de cliente para conectar con la red inalámbrica se pueden conectar con el WGB a través del acceso de Ethernet. El WGB se asocia al AP raíz a través de la interfaz inalámbrica. De esta manera, los clientes atados con alambre consiguen el acceso a la red inalámbrica.

Esta característica proporciona la segregación del tráfico basada en los VLA N para diversas aplicaciones que se ejecutan en diversos dispositivos conectados con un Switch detrás de un

WGB. El tráfico de los clientes WGB será enviado en el priority queue derecho en el regreso de la malla basado en los valores DSCP/dot1p.

Hasta 16 VLA N se soportan para los clientes atados con alambre detrás del WGB.

Nota: Usted necesita una imagen autónoma especial en los AP autónomos que son utilizados como WGB para la Interoperabilidad con la infraestructura unificada CAPWAP. Esta imagen será combinada con la versión autónoma oficial siguiente. Esta característica no está disponible para el MRZ.

WGB y VLAN múltiples

El WGB informa al WLC sobre la información de VLAN del atar con alambre-cliente en el mensaje de la asociación IAPP. El WGB quita la encabezado 802.1q del paquete mientras que envía al WLC. El WLC enviará el paquete al WGB sin la etiqueta 802.1q y el WGB agrega la encabezado 802.1q hacia el Switch atado con alambre, sobre la base de la dirección MAC del destino.

El WLC tratará al cliente WGB como cliente VLAN y remitirá el paquete en la interfaz VLAN correcta basada en el MAC Address de origen

El cliente unificado WGB tiene que ser habilitado para el soporte del VLAN múltiple en el WGB. Esto se inhabilita por abandono.

```
WGB(config)#workgroup-bridge unified-vlan-client
```

Usted tiene que configurar las subinterfaces en el WGB correspondiente a los VLA N en los puertos del switch a los cuales ató con alambre a los clientes están conectados.

Puntas a recordar antes de configurar

- La interfaz dinámica se debe crear en el regulador para cada VLA N configurado en el WGB.
- Solamente una red inalámbrica (WLAN) (SSID) para la asociación de red inalámbrica del WGB a la infraestructura AP se soporta. Este SSID se debe configurar como infraestructura SSID y se debe asociar al VLAN nativo. El WGB caerá todo que no está en el VLAN nativo hacia la infraestructura de la malla.
- El WGB leerá el puerto del switch detrás como cliente en su tabla de la dirección MAC.
- Se recomienda para configurar el mismo VLAN nativo en el WLC de conexión del puerto del switch, WGB, y en el Switch detrás del WGB.Todos los clientes del VLAN nativo en el lado Ethernet WGB serán parte del mismo VLA N en el cual el WGB asscoicated. El WGB será parte del VLA N al cual se asocia la red inalámbrica (WLAN) (en qué WGB se ha asociado).Por ejemplo, si un WGB radio 5 gigahertz (dot11radio 1) se asocia a un VLAN nativo 184, y el Switch detrás del WGB ha atado con alambre a los clientes solamente en el VLA N 185 y 186, después usted no puede requerir el VLAN nativo en el puerto del switch ser idéntico al VLAN nativo en el WGB (VLA N 184). Sin embargo, Cisco le recomienda siempre configura el mismo VLAN nativo en el puerto del switch que el VLAN nativo del WGB.**VLAN nativos no idénticos** Inversamente, si usted agrega a 1 cliente atado con alambre en el VLA N 184, y este cliente VLAN en el WGB pertenece al VLAN nativo, usted tiene que definir el mismo VLAN nativo en el Switch.**El mismo VLAN nativo**
- la movilidad de la Inter-subred se soporta con esta característica para los clientes VLAN detrás del WGB con una limitación que, interfaz dinámica para todos los VLA N del WGB se deba configurar en todos los reguladores.
- La interoperabilidad con la característica de VLA N-reunión no se soporta. Cuando se habilita

la característica de VLA N-reunión, el WGB y sus clientes del VLAN nativo serán parte del mismo VLA N.
- la AAA-invalidación para los clientes WGB no se soporta. Sin embargo, la AAA-invalidación para el WGB se soporta.
- Solamente el Multicast de la capa 3 se proporciona para los clientes VLAN WGB y no hay soporte para el Multicast de la capa 2.
- Hay limitación de 20 clientes en el WGB y clientes de red inalámbrica se incluye en este número.
- La prueba del link para el cliente atado con alambre WGB no se soporta.
- La itinerancia se soporta para la Tecnología inalámbrica y los clientes atados con alambre detrás del WGB.
- El Multicast se soporta para los clientes atados con alambre detrás del WGB
- Se soporta el broadcast.

Diagrama de la red

Configuración vía el CLI en WGB (ejemplo)

En este ejemplo, los VLA N 184 y 185 existen en el Switch atado con alambre detrás del WGB. El VLAN nativo WGB es 184. El SSID es auto-**WGB** maped al VLAN nativo 184. La radio de la radio 1 (5 gigahertz) se está utilizando para conectar con la infraestructura CAPWAP usando este SSID.

```
ap#config t ap(config)#workgroup-bridge unified-vlan-client ap(config)#int FastEthernet0.184
ap(config-subif)#encapsulation dot1q 184 native ap(config-subif)#bridge-group 1 ap(config-
subif)#exit ap(config)#int FastEthernet0.185 ap(config-subif)#encapsulation dot1q 185 ap(config-
subif)#bridge-group 185 ap(config-subif)#exit ap(config)#int Dot11Radio 1.185 ap(config-
subif)#encapsulation dot1q 185 ap(config-subif)#bridge-group 185 ap(config-subif)#exit
ap(config)#int Dot11Radio 1.184 ap(config-subif)#encapsulation dot1q 184 native ap(config-
subif)#bridge-group 1 ap(config-subif)#exit ap(config)#dot11 ssid auto-wgb ap(config-
ssid)#authentication open ap(config-ssid)#infrastructure-ssid ap(config-ssid)#vlan 184
ap(config-ssid)#exit ap(config)#int Dot11Radio 1 ap(config-if)#station-role workgroup-bridge
ap(config-if)#ssid auto-wgb ap(config-if)#exit ap(config)#bridge irb ap(config)#hostname WGB
```

el bridge irb se utiliza para habilitar los Ruteo y Bridging integrados; algo que el código auto AP ha conservado de otras Plataformas más de gama alta.

Uno tiene que crear las interfaces dinámicas 184 y 185 en el WLC para que la configuración antedicha trabaje. El WGB pondrá al día el WLC sobre la información de VLAN del atar con alambre-cliente en el mensaje de la asociación IAPP. El WLC tratará al cliente WGB como cliente VLAN y remitirá el paquete en la interfaz VLAN correcta basada en el MAC Address de origen. En la dirección ascendente, el WGB quitará la encabezado 802.1q del paquete mientras que envía al WLC. En la dirección descendente, el WLC enviará el paquete al WGB sin la etiqueta 802.1q y el WGB agregará la encabezado 802.1q basada en la dirección MAC del destino, mientras que remite el paquete al Switch que conecta al atar con alambre-cliente.

Salida del Bridge WGB

```
WGB#sh bridge Total of 300 station blocks, 292 free Codes: P - permanent, S – self Bridge Group
1: Address Action Interface Age RX count TX count 0023.049a.0b12 forward Fa0.184 0 2 0
0016.c75d.b48f forward Fa0.184 0 21 0 0021.91f8.e9ae forward Fa0.184 0 110 16 0017.59ff.47c2
forward Vi0.184 0 23 22 0021.5504.07b5 forward Fa0.184 0 18 6 0021.1c7b.38e0 forward Vi0.184 0 6
0 Bridge Group 185: 0016.c75d.b48f forward Fa0.185 0 10 0 001e.5831.c74a forward Fa0.185 0 9 0
```

Detalle WGB en el regulador

```
(Cisco Controller) >show wgb summary Number of WGBs..................................... 2 MAC
Address IP Address AP Name Status WLAN Auth Protocol Clients ----------------- --------------- -
---------------- --------- ---- ---- --- 00:1d:70:97:bd:e8 9.47.184.54 c1240 Assoc 2 Yes 802.11a
2 00:1e:be:27:5f:e2 9.47.184.55 c1240 Assoc 2 Yes 802.11a 5 (Cisco Controller) >show client
summary Number of Clients.............................. 7 MAC Address AP Name Status
WLAN/Guest-Lan Auth Protocol Port Wired 00:00:24:ca:a9:b4 R14 Associated 1 Yes N/A 29 No
00:24:c4:a0:61:3a R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:61:f4 R14 Associated 1 Yes
802.11a 29 No 00:24:c4:a0:61:f8 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:0a R14
Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:42 R14 Associated 1 Yes 802.11a 29 No
00:24:c4:a0:71:d2 R14 Associated 1 Yes 802.11a 29 No (Cisco Controller) >show wgb detail
00:1e:be:27:5f:e2 Number of wired client(s): 5 MAC Address IP Address AP Name Mobility WLAN Auth
----------------- --------------- ----------------- ---------- ---- ---- 00:16:c7:5d:b4:8f
Unknown c1240 Local 2 No 00:21:91:f8:e9:ae 9.47.184.83 c1240 Local 2 Yes 00:21:55:04:07:b5
9.47.184.66 c1240 Local 2 Yes 00:1e:58:31:c7:4a 9.47.185.75 c1240 Local 2 Yes 00:23:04:9a:0b:12
Unknown c1240 Local 2 No WGB_1#sh ip int brief Interface IP-Address OK? Method Status Protocol
BVI1 9.47.184.55 YES DHCP up up Dot11Radio0 unassigned YES unset admindown down Dot11Radio1
unassigned YES TFTP up up Dot11Radio1.184 unassigned YES unset up up Dot11Radio1.185 unassigned
YES unset up up FastEthernet0 unassigned YES other up up FastEthernet0.184 unassigned YES unset
up up FastEthernet0.185 unassigned YES unset up up Virtual-Dot11Radio0 unassigned YES TFTP up up
Virtual-Dot11Radio0.184 unassigned YES unset up up Virtual-Dot11Radio0.185 unassigned YES unset
up up
```

Consejos de Troubleshooting

Si un cliente WGB no se está asociando al WGB, estos pasos se pueden utilizar para resolver problemas:

1. El VLAN nativo configurado en el WGB necesita ser lo mismo en el puerto del switch con el cual el WGB está conectado. El puerto del switch conectado con el WGB debe ser trunk.
2. Verifique la configuración del cliente y aseegurese la configuración del cliente es apropiado.
3. Marque la salida del **Bridge de la demostración** en el AP autónomo y confirme que el AP está leyendo el MAC Address del cliente en la interfaz correcta.
4. Confirme las interfaces sub correspondiente a los VLAN determinados y diversas interfaces del submarino se asocian al Grupo de Bridge.
5. Si procede, borre la entrada del Bridge usando el **comando clear bridge** (recuerde este comando quitará a toda la haber atado con alambre y clientes de red inalámbrica asociados en el WGB y hará que se asocian otra vez).
6. El WGB tiene una limitación 20-client, así que aseegurese le no haber excedido el límite.
7. Hasta 16 VLA N se soportan para los clientes atados con alambre detrás del WGB.

QoS en la infraestructura de la malla

Cisco soporta 802.11e en el Acceso local y en el regreso. Los mapas dan prioridad al tráfico de usuarios basado en la clasificación y por lo tanto todo el tráfico de usuarios se trata sobre una base de mejor esfuerzo.

Los recursos disponibles para los usuarios de la malla varían, según la ubicación dentro de la malla, y una configuración que proporciona la limitación de ancho de banda en una punta de la red puede dar lugar al oversubscription en otras partes de la red.

Semejantemente, la limitación de los clientes en su porcentaje del RF no es conveniente para los clientes de la malla. El recurso limitador es no el red inalámbrica (WLAN) del cliente, sino los recursos disponibles en el regreso de la malla. Similar a las redes de los Ethernetes de cable, el 802.11 WLAN emplea el acceso múltiple de la detección de portadora (CS A), pero en vez de usar la detección de colisiones (CD), los WLAN utilizan la Prevención de colisión (CA). Esto

significa que en vez de cada estación que intenta transmitir tan pronto como el media esté libre, los dispositivos WLAN utilizarán un mecanismo de la Prevención de colisión para evitar que las estaciones múltiples transmitan al mismo tiempo.

El mecanismo de la Prevención de colisión utiliza dos valores, llamados aCWmin y aCWmax. Ventana de contención de la significa CW. El CW determina qué cantidad adicional de tiempo debe esperar un punto final, después del espacio interframe (IF), intentar transmitir un paquete. La función distribuida aumentada de la coordinación (EDCF) es un modelo que permite los dispositivos extremos que tienen tráfico de los multi-media de la retrasa sensible para modificar sus valores del aCWmin y del aCWmax para tener en cuenta el acceso estáticamente mayor (y más frecuente) al media.

Soporte de Cisco AP EDCF-como QoS. Esto proporciona hasta ocho colas de administración del tráfico para QoS. Estas colas de administración del tráfico se pueden afectar un aparato en varias maneras diferentes:

- De acuerdo con el TOS/las configuraciones del DiffServ de los paquetes.
- De acuerdo con las Listas de acceso de la capa 2 o de la capa 3.
- De acuerdo con el VLA N.
- De acuerdo con el registro dinámico de los dispositivos (Teléfonos IP).

El Cisco Aironet 1520, conjuntamente con los reguladores de Cisco, proporciona una capacidad de Servicios integrados mínima en el regulador, en el cual las secuencias del cliente tienen casquillos del ancho de banda máximo, y una capacidad más robusta de los Servicios diferenciados (DiffServ) basada en los valores IP DSCP y la red inalámbrica (WLAN) QOS reemplaza.

Cuando se ha alcanzado la capacidad de la cola, se caen las tramas adicionales (eliminación de cola).

‘Encapsulación

Hay varias encapsulaciones usadas por el sistema de malla. Éstos incluyen el control y los datos CAPWAP entre el regulador y el RAP, sobre el regreso de la malla, y entre el MAPA al cliente. La encapsulación del tráfico del bridging (tráfico del NON-regulador de un LAN) sobre el regreso es lo mismo que la encapsulación de los datos CAPWAP.

Hay dos encapsulaciones entre el regulador y el RAP. El primer está para el control CAPWAP, y el segundo para los datos CAPWAP. En el caso del control, CAPWAP se utiliza como envase para la información de control y las directivas. En el caso de los datos CAPWAP, el paquete entero, incluyendo los Ethernetes y los encabezados IP, se envía en el envase CAPWAP (véase las encapsulaciones).

Encapsulaciones

Para el regreso, hay solamente un tipo de encapsulación, encapsulando el tráfico de la malla. Sin embargo, encapsulan a dos tipos de tráfico: interligar el tráfico y control y tráfico de datos CAPWAP. Encapsulan a ambos tipos de tráfico en una encabezado propietaria de la malla.

En el caso del tráfico del bridging, la trama Ethernet entera del paquete se encapsula en la encabezado de la malla (véase el encapsulado del tráfico de la malla).

Todas las tramas del regreso se tratan idénticamente, sin importar si son MAPA A ASOCIAR, A GOLPEAR PARA ASOCIAR, o A ASOCIAR PARA GOLPEAR.

Encapsulado del tráfico de la malla

En el caso del bridging, se transmiten las tramas mientras que se reciben en el ingreso al acceso de Ethernet AP.

Espera en los AP

El AP utiliza un CPU de alta velocidad para procesar las tramas del ingreso, los Ethernetes, y la Tecnología inalámbrica en primero-viene base del primero-servicio. Éstos se hacen cola para la transmisión al dispositivo de salida apropiado, los Ethernetes o Tecnología inalámbrica. Las tramas de salida pueden ser destinadas para el Client Network del 802.11, la red de retroceso del 802.11, o los Ethernetes.

El Cisco Aironet de la serie 1520 AP soporta cuatro (Primero en Entrar, Primero en Salir FIFO) para las transmisiones del cliente de red inalámbrica. Estos (Primero en Entrar, Primero en Salir FIFO) corresponden al platino 802.11e, al oro, a la plata, y a las colas de administración del tráfico del bronce, y obedecen las reglas de la transmisión 802.11e para esas colas de administración del tráfico. Los (Primero en Entrar, Primero en Salir FIFO) tienen una profundidad de espera en cola configurable del usuario.

Asimismo, el regreso (tramas destinadas para otro Punto de acceso al aire libre) utiliza cuatro (Primero en Entrar, Primero en Salir FIFO), aunque el tráfico de usuarios se limita al oro, a la plata, y al bronce. La cola del platino se utiliza exclusivamente para el tráfico de control y la Voz CAPWAP, y se ha vuelto a trabajar de los parámetros estándar 802.11e para CWMIN, CWMAX, y así sucesivamente, para proporcionar una transmisión más robusta pero las latencias más altas.

Semejantemente, los parámetros 802.11e para CWMIN, CWMAX, y así sucesivamente, para la cola del oro se han vuelto a trabajar para proporcionar un tiempo de espera más bajo a expensas de un índice de errores y de una agresividad levemente más altos. El propósito de éstos cambia es proporcionar un canal más conducente a los aplicación de video.

Los capítulos destinados para los Ethernetes se hacen cola como (Primero en Entrar, Primero en Salir FIFO), hasta el disponible máximo transmiten a los recursos compartidos del almacén intermedio (tramas 256). Hay un soporte para el Differentiated Services Code Point IP de la capa 3 (DSCP), así que la marca de los paquetes está allí también.

(En el regulador PARA GOLPEAR la trayectoria para el tráfico de datos, el valor externo DSCP se fija al valor DSCP del bastidor del IP entrante. Si la interfaz está en el modo marcado con etiqueta, el regulador fija el 802.1Q VLAN ID, y deriva el 802.1p PARA ARRIBA (externo) de 802.1p ENCIMA de entrante y del techo de la prioridad predeterminada de la red inalámbrica (WLAN). Los capítulos con VLAN ID 0 no serán marcados con etiqueta (véase el regulador PARA GOLPEAR la trayectoria).

Regulador PARA GOLPEAR la trayectoria

Para CAPWAP, el tráfico de control al valor IP DSCP se fija a *46*, y la prioridad de usuario 802.1p se establece a *7.* antes de la transmisión de una trama de red inalámbrica sobre el regreso, sin importar emparejar del nodo (RAP/MAP) o la dirección, el valor DSCP en el encabezado exterior se utiliza para determinar una prioridad del regreso. Las secciones siguientes describen la asignación entre los cuatro que el regreso hace cola las aplicaciones AP y los valores DSCP mostrados en el trayecto de redireccionamiento QoS.

Tabla 4: Trayecto de redireccionamiento QoS

Valor DSCP	Cola del regreso
2, 4, 6, 8-23	Bronce
26, 32-63	Oro
46-56	Platino
Todos los demás, incluyendo 0	Plata

Nota: La cola del regreso del platino es reservada para el tráfico de control CAPWAP, el tráfico de control IP, y los paquetes de voz. El DHCP, el DNS y los pedidos ARP también se transmiten en el nivel de QoS del platino. El software de la malla examina cada trama para determinar si es un control CAPWAP o trama de control IP para proteger la cola del platino contra el uso por las aplicaciones NON-CAPWAP.

Para un MAPA a la trayectoria del cliente, hay dos diversos procedimientos, dependiendo de si el cliente es un cliente WMM o un cliente normal. Si el cliente es un cliente WMM, el valor DSCP en la trama externa se examina, y se utiliza el priority queue 802.11e (véase el MAPA a la trayectoria QoS del cliente).

Cuadro 5: MAPA a la trayectoria QoS del cliente

Valor DSCP	Cola del regreso
2, 4, 6, 8-23	Bronce
26, 32-45, 47	Oro
46, 48-63	Platino
Todos los demás, incluyendo 0	Plata

Espera en los AP

Si el cliente no es un cliente WMM, la invalidación WLAN (según lo configurado en el regulador) determina la cola 802.11e (bronce, oro, platino, o plata), en la cual se transmite el paquete.

Para el cliente hacia el AP, hay modificaciones hechas a las tramas del cliente entrante con objeto de la transmisión en el regreso o los Ethernetes de la malla. Para los clientes WMM, el MAPA ilustra la manera de la cual el valor externo DSCP se fija de una trama entrante del cliente WMM.

MAPA PARA GOLPEAR la trayectoria

El mínimo de la prioridad de usuario entrante 802.11e y de la prioridad de la invalidación WLAN se traduce usando la información enumerada adentro para determinar el valor DSCP del bastidor IP. Por ejemplo, si la trama entrante tiene como su valor una prioridad que indica la prioridad del oro, solamente el WLAN se configura para la prioridad de plata, la prioridad mínima de la plata se utiliza para determinar el valor DSCP.

Cuadro 6: DSCP al mapeo de cola del regreso

Valor DSCP	802.11e PARA ARRIBA	Cola del regreso	Tipos de paquete
2, 4, 6, 8 - 23	1, 2	Bronce	Los paquetes prioritarios más bajos si ninguno

26, 32-34	4, 5	Oro	Paquete de video
46 - 56	6, 7	Platino	Control CAPWAPP, AWPP, DHCP/DNS, paquetes ARP, paquetes de voz
Todos los demás, incluyendo 0	0, 3	Plata	Mejor esfuerzo, paquetes de datos CAPWAPP

En caso que no haya prioridad entrante WMM, la prioridad predeterminada de la red inalámbrica (WLAN) se utiliza para generar el valor DSCP en el encabezado exterior. En caso que la trama sea una trama de control originada CAPWAP, el valor DSCP de 46 se pone en el encabezado exterior.

Con las 5.2 mejoras del código, la información DSCP se preserva en la encabezado AWPP.

Todo el tráfico atado con alambre del cliente se restringe a un máximo 802.1p ENCIMA del valor de 5, a menos que DHCP/DNS y los paquetes ARP, ellos pasen a través de la cola del platino.

El tráfico del cliente de red inalámbrica NON-WMM consigue el valor por defecto prioridad de Calidad de servicio (QoS) de su red inalámbrica (WLAN). Mientras que, el tráfico del cliente de red inalámbrica WMM puede tener el valor máximo 802.11e de 6, pero los debe estar debajo del perfil de QoS configurado para su red inalámbrica (WLAN). Si se configura el control de admisión, los clientes WMM deben utilizar la señalización TSPEC y conseguir admitidos por el CAC.

El tráfico de datos CAPWAPP lleva el tráfico del cliente de red inalámbrica y por lo tanto tiene la misma prioridad y tratamiento que el tráfico del cliente de red inalámbrica.

Ahora que se determina el valor DSCP, las reglas descritas anterior para el trayecto de redireccionamiento del RAP PARA ASOCIAR se utilizan para determinar más lejos la cola del regreso en la cual se transmite la trama. Los capítulos transmitidos del RAP al regulador no se marcan con etiqueta. Los valores externos DSCP se dejan intactos, pues primero fueron construidos.

Interligar los paquetes de retroceso

Interligando los servicios se tratan un poco diferentemente de los servicios regulador-basados regulares. No hay valor externo DSCP en los paquetes del bridging porque no son CAPWAP encapsulados. Por lo tanto, el valor DSCP en el encabezado IP como fue recibido por el AP se utiliza para poner en un índice en la tabla según lo descrito en la trayectoria del AP a AP (regreso).

Interligando los paquetes y a un LAN

Los paquetes recibidos de una estación en un LAN no se modifican de ninguna manera. No hay valor de la invalidación para la prioridad LAN. Por lo tanto, en el Bridging Mode el LAN debe ser asegurado correctamente. La única protección ofrecida al regreso de la malla es que las tramas de control NON-CAPWAP que asocian a la cola del platino están degradadas a la cola del oro.

Los paquetes se transmiten al LAN exacto mientras que se reciben en el ingreso en los

Ethernetes de la entrada a la malla.

La única forma de integrar QoS entre los accesos de Ethernet en AP1520 y el 802.11a está marcando los paquetes Ethernet con etiqueta con el DSCP. El AP1520 tomará el paquete Ethernet con el DSCP y lo colocará en la cola apropiada 802.11e.

Los 1520 no marca DSCP con etiqueta sí mismo:

- En el puerto de ingreso, los 1520 ve una etiqueta DSCP y encapsularán la trama Ethernet y aplicarán la prioridad correspondiente 802.11e.
- El en el puerto de egreso, los 1520 decapsulates la trama Ethernet y la pone en el alambre con un campo sin tocar DSCP.

Los dispositivos Ethernet, como los cámara de video, deben tener la capacidad para marcar los bits con el valor DSCP para aprovecharse de QoS.

Instalación WGB

Un AP en el modo WGB está instalado en el tren o el vehículo móvil. Este AP conectará con la red de la infraestructura de red inalámbrica a lo largo de las vías o el camino en una moda Lineal. El WGB hará rápidamente la itinerancia y mantendrá la Conectividad si todas las configuraciones necesarias se hacen en la infraestructura WGB y AP.

Ejemplo móvil del tren

Aquí también, es recomendable ir con la antena direccional para un mejor uso de la energía RF. Las Antenas de la corrección son preferibles en este caso pues no será afectado por la resistencia del viento en los trenes rápidos.

Los trenes se sujetan regularmente a lavarse con los chorros de agua y las sustancias químicas y si el WGB AP se monta afuera, pueden conseguir dañados. Los trenes también se ejecutan en las velocidades, así que es importante elegir la antena que se significa para el aire libre y puede soportar las velocidades de un fuerte viento. Los fuertes vientos pueden destrozar la antena si están montados afuera.

La potencia de la señal baja acciona a un cliente de WiFi que vaga por típicamente, una subida de las consideraciones de la tarifa de error de paquete, o del cargamento AP. En el caso antedicho, cuando el AP está actuando en el jefe del tren, la señal de WiFi en el WGB ganará en la potencia de la señal como el tren se mueve más cercano al AP, después los cambios de la señal del estado más fuerte al estado más débil en la punta AP vagan por. Esto retrasará la época AP de hacer la itinerancia.

Cuando el WGB se monta en la cola del coche de tren, la señal de WiFi en el WGB ganará en la fuerza como el tren se mueve lejos del AP que se asocia a. Los cambios de la señal del estado más débil al estado más fuerte en la punta AP vagan por y éste permite al AP para tomar la decisión de itinerancia más rápidamente.

Tren AP

Por lo tanto, es recomendable montar el tren AP en la cola del tren.

La diversidad es un aspecto importante de conseguir más aumento. Uno debe intentar conseguir la ventaja máxima de él — como el más el presupuesto del link en el uplink, mejor es el funcionamiento. Eligió una antena que tiene dos puertos de entrada y puede honrar los puertos de

la diversidad que vienen de los AP. Aseegurese utilizar los cables de pequeñas pérdidas que conectan la antena y el Punto de acceso. Si usted está utilizando la antena del puerto único, después aseegurese por favor que usted ha conmutado de la diversidad, pues la diversidad con la sola antena puede crear condiciones peores.

La figura siguiente muestra a 13 dBi la antena externa 5 gigahertz con dos puertos, de Huber+Suhner con 30 grados de vertical y los anchos de banda horizontales. La antena se monta en la parte de posterior el coche. Por supuesto, si la misma serie se está moviendo en la dirección del norte y sur que dos WGB se pueden instalar en cada coche/coche del tren en dos finals del extremo. Esto no sólo aumentará la Redundancia, pero también aumenta la capacidad de acomodar a los clientes, como un solo WGB puede asociar solamente a 20 clientes mientras que habla con una infraestructura unificada AP.

13 dBi antena externa 5 gigahertz 13 dBi antena externa 5 gigahertz montada en el coche

Si el montaje de la antena fuera del vehículo móvil no es posible, después las Antenas se pueden afianzar con abrazadera o reparar típicamente al revestimiento de cristal afuera delante del tren. La pantalla de cristal en el tren puede inducir una pérdida de DB 2-4 dependiendo del espesor. La antena debe tener bastante aumento para compensar esa pérdida.

Antenas montadas al vidrio

A veces, las vías del tren pueden tener líneas de potencia alta por encima (hasta 4,000 vatios). Estos trenes se fugan la energía eléctrica, en vez del carbón o del diesel. Aunque estas líneas de energía11 no creen interferencia RF, crean los requisitos que ponen a tierra especiales para las Antenas que van en los tejados del tren. Muchos vendedores como Huber+Suhner se especializan en proporcionar a las Antenas del tren que cumplen estos requisitos.

Para instalar un WGB, proceda siempre con “fuera del sitio fuera un acercamiento de la mente” a evitar el vandalismo. Un WGB dentro del tren tiene que proporcionar la cobertura para 2.4 gigahertz del acceso. Como consecuencia, el cuidado apropiado se debe tomar para instalar estas Antenas de una manera sin obstáculo. La imagen siguiente muestra una un tal instalación en una de la esquina dentro de un coche del tren dentro del tejado. Se oculta y no es totalmente visible. Dos cables de pequeñas pérdidas RF se han tomado afuera de los dos puertos de antena de AP1242 y se han asociado a la antena de tercera persona externa. Esta imagen muestra a un corte transversal del coche del tren donde el AP1242 WGB ha estado instalado:

Corte transversal del coche del tren

Este corte transversal se cubre realmente con la cubierta metálica que corresponde con la estructura corporal interna del coche exactamente.

Observe que el acceso al cliente se puede también hacer disponible para los pasajeros o los clientes que se colocan en la plataforma, esperando la estación etc, pues la infraestructura del MAPA está ya allí. Como consecuencia, el acceso al cliente se puede proporcionar en 5 gigahertz y 2.4 gigahertz directamente de los mapas. Ahora los clientes se moverán desde el (WGB) autónomo CAPWAP unificado AP (malla) AP. ¡La bueno parte de este acceso al cliente es que no requiere rápidamente la itinerancia! Otra bueno parte es que un presupuesto del link fuerte está disponible no sólo en la dirección del link descendente debido a la potencia alta, pero también en la dirección del uplink debido a las Antenas múltiples. Para 2.4 gigahertz del acceso al cliente directamente de los mapas, la relación de transformación máxima que combina (MRC) se puede utilizar para aprovecharse de aumentos más altos del receptor. Al actuar con las velocidades de datos más altas que 12 Mb/s, usted pueden aumentar el aumento en una radio 2.4-GHz a DB 2.7 agregando 2 Antenas y a DB 4.5, agregando 3 Antenas.

Usted también tiene que marcar en cuanto a cuánto voltaje está disponible en el tren o el vehículo móvil. Las medidas de la tercero-parte tienen que ser tomadas a veces para subir al convertido o abajo para convertir el voltaje disponible para accionar encendido el WGB. Generalmente en el USA, 72V está disponible en el tren, así que los convertidores de la tensión de CC 72-48V tienen que ser instalados y los cables se han funcionado con internamente para que a cada coche traiga la alimentación eléctrica de CC 72V del motor del tren a cada coche.

Router de acceso móvil

Las Cisco 3200 Series MARCHA consisten en 1 o más módulo PC104/Plus que empilan juntos para formar una configuración del router inalámbrico. Estas combinaciones de la placa modular son cualquiera disponible como conjuntos del indicador luminoso LED amarillo de la placa muestra gravedad menor o como sistemas completos ensamblados en un recinto rugoso de Cisco 3200.

Cisco 3200 Series MARCHA

La opción rugosa del recinto de Cisco para las 3200 Series se diseña para el uso del en-vehículo, dirigiendo las necesidades específicas de la movilidad de la seguridad pública, el transporte, la defensa, y los mercados de la seguridad de la patria. La opción rugosa del recinto se sella y se diseña totalmente para soportar los entornos duros, incluyendo las variaciones grandes en la temperatura y la altitud, el choque intenso/la vibración, y la exposición a la humedad, a la humedad, o al polvo.

Refiera por favor a la hoja de datos de los recintos del Routers resistentes de servicios integrados Cisco de la serie 3200 para más información y fomente los detalles del recinto rugoso.

Los conjuntos del Cisco 3200 Series Router consisten en Cisco 3230 y Cisco 3270 modelos. El conjunto consiste en un indicador luminoso LED amarillo de la placa muestra gravedad menor móvil del router de acceso (MARC), una tarjeta de interfaz móvil serial (SMIC), un fast ethernet conmutando la tarjeta de interfaz móvil (FESMIC), las tarjetas de interfaz móviles inalámbricas (WMICs) y un indicador luminoso LED amarillo de la placa muestra gravedad menor del poder del router móvil (MRPC).

Para su referencia, muestran el conjunto MAR3230 aquí:

Para más información sobre Cisco 3200 conjuntos del indicador luminoso LED amarillo de la placa muestra gravedad menor refieren a la hoja de datos rugosa del Routers de los Servicios integrados de Cisco 3230.

MARC

MARC es un router IOS 3250:

Incluye el procesador host, la memoria, y las encabezados para los fast ethernet, la consola, y las señales auxiliares para el router.

1: BUS PCI, 2: BUS ISA, 3: Fast ethernet, 4: Encabezado multifuncional

El conector del bus PCI soporta la comunicación entre el SMIC, el FESMIC, y MARC. El WMIC comunica con el router a través de un puerto Fast Ethernet interno y se configura a través de un puerto de la consola independiente; el WMIC extrae solamente el poder del bus.

FESMIC

El FESMIC es un switch Fast Ethernet 4-port:

1: BUS PCI, conector 2:LED, 3: BUS ISA, 4: Switch rotatorio, encabezados Ethernet 5-8:Fast.

La posición del Switch rotatorio determina las asignaciones de puertos. La posición rotatoria para el MARCHA instalado respecto a los busses será 2, que corresponde a los fast ethernet 2/0-2/3. El indicador luminoso LED amarillo de la placa muestra gravedad menor comunica a MARC a través del bus PCI.

WMIC

Hay tres tipos de WMICs, dependiendo de la banda de frecuencia:

- gigahertz de la tarjeta de interfaz 5 del “802.11a” (C3205WMIC-TPEK9)
- “802.11bg” gigahertz de la tarjeta de interfaz 2.4 (C3201WMIC-TPEK9)
- gigahertz de la tarjeta de interfaz 4.9 del “802.11a” (C3202WMIC-TPEK9)

Hay 2 de ellos en el MARCHA de 3230.

Pueden ser configurados como WGB. El WGB es similar a un cliente AP:

Permitirá que el MARCHA conecte con la infraestructura AP a lo largo de la pista/del ferrocarril o del interior el túnel, el etc.

1: BUS PCI, 2: Antena izquierda, 3: Antena derecha, 4: BUS ISA, 5: Fast ethernet, 6: Conector LED y de la consola.

El WMIC no utiliza el bus PCI y ISA. Comunica con el router a través de un puerto Fast Ethernet interno.

SMIC

El SMIC proporciona al router con hasta cuatro conjuntos de alta velocidad de las señales seriales en el equipo de terminal de datos (DTE) y los modos del equipo del circuito de datos (DCE):

1: BUS PCI, 2: encabezado multifuncional 60-pin para las señales del serial0 y del Serial1, 3: BUS ISA, 4: Switch rotatorio

El conector del bus PCI soporta la comunicación entre el SMIC y MARC. La posición del Switch rotatorio determina las asignaciones de puertos. Aunque el Switch rotatorio tenga 8 posiciones, sólo la posición 0, 1, y 2 se soporta respecto al 4-port SMIC.

MRPC

El MRPC:

El indicador luminoso LED amarillo de la placa muestra gravedad menor del poder DC/DC es haber construido sólidamente, específico a la aplicación, triple-salida, PC/104 — convertidor Más-compatible. Valida las entradas 12-VDC o 24-VDC de un sistema de batería del vehículo y proporciona las salidas completamente protegidas 3.3V, 5V, y 12V. El adaptador de energía

AC/DC proporciona un compatible entrada de CC al no ser utilizado en una aplicación 12-VDC o 24-VDC.

Los 3200 tiene interfaces múltiples:

- Las interfaces de Ethernet se utilizan para conectar a cualquier cliente atado con alambre en-vehículo, tal como laptop, cámara, o dispositivos de la telemática con la red.
- Las interfaces seriales proporcionan la Conectividad a los módems PÁLIDOS inalámbricos que conectan con las redes celulares tales como CDMA o GPRS.
- WMIC se configura como WGB para la Conectividad a las redes inalámbricas.

La ventaja de usar MAR3200 es que puede dar la Conectividad de reserva sobre las redes celulares tales como GPRS o CDMA. Las conexiones inalámbricas del 802.11 se tratan como servicios preferidos porque ofrecen la mayoría del ancho de banda. Sin embargo, cuando una conexión de la red inalámbrica (WLAN) no está disponible, la tecnología celular proporciona un link de backup. La prioridad de la conexión puede ser establecida ruteando la prioridad o por la prioridad para el IP móvil.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems