Troubleshooting Básico de Hybrid Remote Edge Access Point (H-REAP)

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Troubleshooting H-REAP
H-REAP no se une al WLC
Verificación del modo de operación H-REAP
Los comandos console de H-REAP no son operativos y vuelven un error
Los clientes no pueden conectar con H-REAP
Cuentas incorrectas del cliente de los informes inalámbricos del sistema de control (WCS) al AP en el modo H-REAP
Información Relacionada

Introducción

Hybrid Remote Edge Access Point (H-REAP) es una solución para la implementación en oficinas y sucursales remotas. Permite a los clientes configurar y controlar dos o tres Puntos de acceso (APs) en una bifurcación o una oficina remota de la oficina corporativa a través de un link del Red de área ancha (WAN) sin la necesidad de desplegar un regulador en cada oficina. Este documento discute algunos de los problemas frecuentes que pueden ocurrir en un entorno H-REAP. Este documento también proporciona a la información en cómo resolver problemas estos problemas. Refiera al diseño y al Guía de despliegue H-REAP para los aspectos del diseño H-REAP cuando usted despliega H-REAP y configurando el híbrido COSECHE para los pasos para la configuración.

prerrequisitos

Requisitos

- Conocimiento funcional de H-REAP y de sus modos de operación
- Conocimiento del proceso de inscripción ligero del Punto de acceso (REVESTIMIENTO) a un regulador
- Conocimiento del protocolo ligero del Punto de acceso (LWAPP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Reguladores inalámbricos LAN de las Cisco y? Series (WLCs) esa versión 5.1 del funcionamiento
- AG 1130AG APs, 1240 APs de Cisco, y 1250 APs
- Cisco 2800 y 3800 Series Router que funcionan con la versión 12.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Éstas son las restricciones a recordar mientras que usted utiliza H-REAP.

- REAP híbrida se utiliza solamente en el 1130AG, los 1140, los 1240, los 1250, los 1260, el AP801, el AP 802, 1040, y el AP3550 APs y en Cisco WiSM, Cisco 5500, 4400, 2100, 2500, los reguladores de las 7500 Series de la flexión, el conmutador inalámbrico integrado 3750G del regulador LAN del catalizador, y el módulo de red del regulador para el Routers de los Servicios integrados.
- Cualquier tipo de la Seguridad que requiera el control sobre la trayectoria de datos, tal como VPN, no trabaja con el tráfico en las redes inalámbricas (WLAN) localmente cambiadas porque el regulador no puede efectuar el control sobre los datos que no se hacen un túnel de nuevo a él. Cualquier otro tipo trabajos de la Seguridad en redes inalámbricas (WLAN) centralmente o localmente cambiadas, a condición de que la trayectoria entre el H-REAP y el regulador está para arriba. Cuando este conducto está abajo, sólo un subconjunto de estas opciones de seguridad permite que los nuevos clientes conecten con las redes inalámbricas (WLAN) localmente cambiadas.
- Cuando un Punto de acceso H-REAP ingresa al modo autónomo, WLANs que se configura para abierto, compartido, WPA-PSK, o WPA2-PSK autenticación ingrese “autenticación local, el estado de la transferencia local” y continúe las nuevas autenticaciones de cliente.En el Software Release 4.2 o Posterior del regulador, esto es también verdad para las redes inalámbricas (WLAN) que se configuran para el 802.1x, WPA-802.1X, WPA2-802.1X, o la administración de claves centralizada Cisco (CCKM). Sin embargo, estos tipos de la autenticación requieren que configuren a un servidor de RADIUS externo. El otro WLANs ingresa “autenticación abajo, cambiando abajo” del estado (si el WLAN fue configurado para la transferencia central) o “autenticación abajo, el estado de la transferencia local” (si el WLAN fue configurado para la transferencia local).
- Con H-REAP en el modo conectado, el regulador está libre de imponer la exclusión del cliente/poner para evitar que algunos clientes se asocien a sus APs. Esta función puede ocurrir en la moda automatizada o manual. Con respecto a las configuraciones globales y de la por-red inalámbrica (WLAN), los clientes pueden ser excluidos para un host de las razones,

que se extienden de los intentos de autenticación fallados relanzados al hurto IP, así como para cualquier cantidad de tiempo determinada. Los clientes también pueden incluirse en esta lista de exclusión manualmente. El uso de esta característica es solamente posible mientras que el AP está en el modo conectado. Los clientes que se han colocado en esta lista de la exclusión siguen siendo incapaces de conectar con el AP, incluso mientras que está en el modo autónomo

- Las redes inalámbricas (WLAN) que utilizan la autenticación MAC (local o contra la corriente) permiten no más las autenticaciones de cliente adicionales cuando el AP está en el modo autónomo, que es idéntico a la manera a la red inalámbrica (WLAN) semejantemente configurada con el 802.1x o WebAuth actúa en el mismo modo.
- Las versiones 4.2.61.0 WLC y la ayuda posterior rápida aseguran la itinerancia usando CCKM. El modo H-REAP utiliza la itinerancia segura de la capa 2 rápidamente usando CCKM. Esta característica previene la necesidad de la autenticación completa RADIUS EAP mientras que el cliente vaga por a partir de un AP a otro. Para utilizar CCKM ayune vagando por con los Puntos de acceso H-REAP, usted necesitan configurar a los grupos H-REAP.

Troubleshooting H-REAP

Algunos escenarios y situaciones impiden la correcta configuración de H-REAP y la conectividad del cliente. Éstas son apenas algunas tales situaciones con sus pasos de troubleshooting sugeridos.

H-REAP no se une al WLC

Éstas son las razones básicas de un H-REAP para no unirse al WLC:

- H-REAP no puede obtener una dirección IP a sí mismo, o se ha asignado con una dirección IP incorrecta.
- No hay ninguna Conectividad layer-3 entre H-REAP y el WLC.
- No hay una Conectividad ligera del protocolo del Punto de acceso (LWAPP) entre el H-REAP y el WLC.
- Otras razones son los H-REAP que se unen a un diverso regulador, a la discordancía del certificado, al problema con WLC o H-REAP sí mismo, al etc.

Realice estos pasos para resolver problemas estos problemas:

1. Verifique que H-REAP AP esté asignado una dirección IP.Si el DHCP se utiliza a través de la consola del AP, verifique que el AP consiga un direccionamiento con este comando:.
   ```
   AP_CLI#show dhcp lease
   ```

   Si la salida de este comando no es ninguna, implica que el direccionamiento DHCP no está utilizado para este AP.Ahora, asegúrese de que la dirección IP estática esté asignada al AP en una forma adecuada. Esto se puede verificar con este comando:
   ```
   AP_CLI#show lwapp ip config
   ```

   ```
   LWAPP Static IP Configuration
   IP Address          10.77.244.222
   IP netmask          255.255.0.0
   Default Gateway     10.77.244.220
   ```

La salida visualiza una dirección IP estática de 10.77.244.222 asignó al AP. Si ésta no es la dirección IP prevista que se asignará, corrija la dirección IP.

2. Verifique la Conectividad IP entre el AP y la interfaz de administración del regulador.Una vez que se ha verificado la dirección IP, haga ping la dirección IP de la Administración del regulador para asegurarse de que el AP puede comunicar con el regulador. Utilice el comando ping a través de la consola del AP con este sintaxis:

```
AP_CLI#ping 10.77.244.210
!--- 10.77.244.210/27 is the example management interface IP address of the controller.
```

Si el ping no es acertado, indica que hay un problema en la Conectividad IP entre el AP y el regulador. Asegúrese de que la red ascendente esté configurada correctamente y de que el acceso a WAN de nuevo a la red corporativa está para arriba. Verifique que el regulador sea operativo y no esté detrás de ningunos límites **NAT/PAT**. Haga ping del regulador al AP con el mismo sintaxis. Asegúrese de que el **MTU** para la trayectoria entre el regulador y el H-REAP esté en un mínimo de **1500**. Esto se puede controlar con el **ping - l 1500 *IP de administración >*** comando *<WLC de un* ordenador en el lado H-REAP de WAN.Aquí está una salida de muestra del comando de ping exitoso:

```
ping -l 1500 10.77.244.210

Pinging 10.77.244.204 with 1500 bytes of data:

Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252

Ping statistics for 10.77.244.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum =  6ms, Average =  6ms
```

3. Verifique la Conectividad LWAPP entre el AP y el regulador.Una vez la Conectividad IP entre el H-REAP y el regulador se ha verificado, realiza las depuraciones LWAPP en el regulador para confirmar que los mensajes LWAPP están comunicados a través de WAN y para identificar los problemas relacionados. En el controlador, cree en primer lugar un filtro MAC para limitar el alcance de la salida de los debugs. Utilice este comando de limitar la salida del comando subsiguiente a un solo AP:

```
AP_CLI#debug mac addr <AP's wired MAC address> .
```

Una vez que esto se fija para limitar la salida de la depuración, gire el depuración LWAPP con este comando:

```
Controller_CLI#debug lwapp events enable
```

Usted ve los mensajes de la depuración similares a éstos:

```
-----------------------------------------------
       -------------------------------------------------
       -------------------------------------------------------
       Thu Mar 15 15:07:56 2007: 00:12:44:b2:ae:d0
Received LWAPP DISCOVERY REQUEST from AP 00:12:44:b2:ae:d0
to ff:ff:ff:ff:ff:ff on port '1'
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Received LWAPP JOIN REQUEST from AP 00:12:44:b2:ae:d0
to 00:0b:85:33:84:a0 on port '1'
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
 AP AP0012.d92b.3a5e: txNonce  00:0B:85:33:84:A0 rxNonce  00:12:44:B2:AE:D0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
LWAPP Join-Request MTU path from AP 00:12:44:b2:ae:d0
is 1500, remote debug mode is 0
```

```
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Successfully added NPU Entry
for AP 00:12:44:b2:ae:d0 (index 50)Switch IP: 10.77.244.211,
Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.10, AP Port: 45989,
        next hop MAC: 0 0:12:d9:2b:3a:5e
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Successfully transmission of LWAPP Join-Reply to AP 00:12:44:b2:ae:d0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
 Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 1
       Thu Mar 15 15:08:08 2007: 00:12:44:b2:ae:d0
Received LWAPP CONFIGURE REQUEST from AP 00:12:44:b2:ae:d0 to  00:0b:85:33:84:a0
       ----------------------------------------------------
       ----------------------------------------------------
       ----------------------------------------------------
```

Esta salida de la depuración indica una transmisión exitosa de los mensajes LWAPP entre el regulador y el AP, seguida por un acertado únase a la petición del AP y el paralelo se une a la contestación del regulador. El AP consigue más adelante registrado con el regulador.Si no se considera ningunos tales mensajes de la depuración LWAPP, asegúrese de que el H-REAP tenga por lo menos un método por el cual un regulador pueda ser descubierto. Si tales métodos existen (como la difusión de la subred local, la opción 43 del DHCP, o el DNS), verifique que estén configurados correctamente. Si no hay otro método de descubrimiento, asegúrese de que el IP address del regulador esté ingresado manualmente en el AP a través de la consola CLI.

```
AP_CLI#lwapp ap controller ip address
  <management interface Ip address of controller>
```

4. Si usted ha configurado manualmente el H-REAP, asegúrese de le información del controlador previamente asociada clara cuando usted mueve su AP a una ubicación diferente en su red. Esto permite que su AP se asocie al regulador en la nueva ubicación. Para borrar la configuración previa, publique el comando de los soldado-**config del lwapp** AP CLI#clear. Entonces, verifique independientemente de si el AP se una al regulador correcto.Para verificar con qué reguladores comunica el AP, publique el **comando debug ip udp al** AP CLI. De la salida de este comando, vea a las direcciones de origen y de destino de cada paquete que atraviese la pila IP del AP.Aquí tiene un ejemplo:**IP UDP de** AP_CLI#debug

```
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=60
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223)
, length=75
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989)
, length=49
*Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=76
*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
```

De esta salida, usted puede ver que los paquetes UDP son originarios del AP y que alcanzan el interfaz de la interfaz de administración (10.77.244.210) y del encargado AP (10.77.244.211) del regulador.

5. Resuelva problemas los problemas del certificado si las tentativas AP de unirse al regulador pero fallan.Si los mensajes LWAPP se consideran en el regulador, pero el AP no puede unirse a, esto es probable un problema del certificado. Para más extremidades de troubleshooting LWAPP, que incluyen los problemas del certificado del troubleshooting,

refiera a las extremidades del Troubleshooting de la herramienta de actualización LWAPP.

6. Otra razón que H-REAP APs no se unen a WLCs es si el proxy ARP se inhabilita en el gateway para el H-REAP APs. De la consola AP, se registra este mensaje:

```
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=60
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223)
, length=75
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989)
, length=49
*Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=76
*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
```

Esto se puede causar por el ID de bug CSCse92856 de Cisco. Este problema se aplica solamente a AP1130 y a AP1240. Este problema no se aplica a AP1000s, al AP1100, o al AP1200.Este problema ocurre cuando se cumplen estas condiciones:El modo HREAP se utiliza en la red inalámbrica (WLAN). El modo local no es afectado por este problema. Se requiere la asignación nativa del VLA N.Los APs tienen que estar en una diversa subred IP que el encargado AP del WLCs.El proxy ARP se inhabilita en el gateway de valor por defecto para el AP.El H-REAP AP consigue el gateway de valor por defecto de un servidor del DHCP.Para resolver este problema, proxy ARP del permiso en el router de gateway del valor por defecto del AP.

Verificación del modo de operación H-REAP

Una vez que el H-REAP se ha unido al regulador correcto, usted puede verificar independientemente de si el H-REAP AP esté conectado con el regulador en cualquier momento. Es decir usted puede verificar en qué modo funciona el H-REAP AP. Esto se puede verificar con el **lwapp de la demostración cosecha el comando status del** AP CLI.

El lwapp de AP_CLI#show **cosecha el estatus**

```
AP Mode:        REAP, Connected
                Radar detected on:
```

Esta salida dice que el H-REAP AP está en el modo H-REAP y el modo conectado. Es decir el link PÁLIDO entre el AP y el regulador está PARA ARRIBA (conectado), y el modo de operación es H-REAP.

El lwapp de AP_CLI#show **cosecha el estatus**

```
AP Mode:        REAP, Standalone
                Radar detected on:
```

Esta salida dice que el AP está en el modo autónomo, así que significa que el link PÁLIDO entre el AP y el regulador está abajo. El modo de operación AP es COSECHA. Esto significa que las redes inalámbricas (WLAN) que se configuran para la transferencia local con la autenticación local son funcionales y permiten a los nuevos clientes a esta red inalámbrica (WLAN). Refiera al ejemplo de la configuración de los modos de operación H-REAP para entender a los diversos modos de operación de H-REAP.

Los comandos console de H-REAP no son operativos y vuelven un error

Cualquier comando de configuración (para establecer o despejar la configuración) realizados a través de la CLI de H-REAP devuelve el mensaje ERROR. El comando está inhabilitado. Esto puede ocurrir para una de dos razones:

- H-REAP APs que están en el modo conectado (registrado al regulador) no permiten que borraas ninguna configuraciones sean fijadas o a través de la consola. Cuando el AP está en este estado, las configuraciones se deben hacer a través del interfaz del regulador. Si el acceso a los comandos configuration en el AP se requiere, asegúrese de que el AP esté en el modo autónomo antes de que usted intente ingresar cualquier comando configuration.
- Una vez que un AP ha conectado o se ha registrado a un regulador en cualquier momento, asegúrese de que la contraseña del permiso del valor por defecto de H-REAP, **Cisco**, esté cambiada. Si esta contraseña de valor por defecto no se cambia, usted no puede tener acceso a la consola CLI del H-REAP se mueve al modo autónomo. La contraseña del permiso se puede fijar solamente con el CLI del regulador con el cual el AP está conectado. Esta sintaxis de ordenes se puede utilizar en el regulador para fijar la contraseña de consola de un AP individual o la contraseña a todos los APs del regulador: Del >config (WLC_CLI) **ap username contraseña *<user-id>* *<passwd>* {todos | name> <AP}**.Aquí tiene un ejemplo:
  ```
  WLC-1>config ap username hreap password hreap all
  ```

  Nota: Si usted está funcionando con la versión 5.0 y posterior WLC, utilice este comando: **el mgmtuser ap de los config agrega el *secreto* secreto del password password del nombre de usuario nombre de usuario {todo | Nombre AP}Nota:** Para un AP que no ha tenido sus contraseñas de consola fijadas, sea consciente que esta configuración está enviada solamente al AP cuando el comando se ingresa en el regulador. Cualquier APs que se una a posteriormente el WLC requiere el comando de ser ingresado otra vez.**Nota:** Trabajo de estos comandos encendido **fuera de - El cuadro H-**cosecha incluso cuando la contraseña de valor por defecto no se cambia:*<name> del* ***hostname ap del lwapp****dirección IP del* ***IP address*** *<AP* ***ap del lwapp*** *> <subnet mask>la dirección IP de los <Gateway del valor por defecto-****gateway IP ap del lwapp*** *>dirección IP del* ***IP address*** *<WLC del* ***regulador ap del lwapp*** **>borre los soldado-config del lwapp**
- **Nota:** Para volver totalmente el AP a los valores por defecto de la fábrica, sobre el cargador del programa inicial AP, presiona el **botón mode** hasta que la luz de los Ethernetes dé vuelta al ámbar. En los 1131, esta luz está cerca del botón mode y se marca claramente con los Ethernetes. En los 1242, esto está bajo la fachada plástica blanca y notated con un E. Release el botón mode y dejó el cargador del programa inicial AP. El AP se vuelve al interfaz, que está disponible con la imagen de recuperación IOS del AP. Sea consciente que si desean a los nuevos comandos configuration, el AP necesita funcionar con el Software Release 12.3(11)JX1 o Posterior de Cisco IOS®. Esto se puede verificar a través de la consola del AP ingresando el **comando show version**.**Nota:** Todos los **comandos show and debug** continúan trabajando sin una contraseña de valor por defecto que es fijada y mientras que el AP está en el modo conectado.A este punto puede cualquier configuración LWAPP ser hecha solamente.

Los clientes no pueden conectar con H-REAP

Si los clientes de red inalámbrica no pueden conectar con H-REAP, realice estos pasos:

1. Asegúrese de que el link PÁLIDO entre el regulador y el H-REAP esté para arriba.
2. Verifique que el AP se haya unido a correctamente el regulador y que el regulador tiene por lo menos una (y activado) red inalámbrica (WLAN) correctamente configurada. Asegúrese de que el **H-REAP** esté en el estado activado para las redes inalámbricas (WLAN) localmente cambiadas
3. En el regulador, configure la red inalámbrica (WLAN) para difundir su SSID para ayudar a resolver problemas este proceso. En el extremo del cliente, verifique si el cliente puede encontrar el AP con el SSID. Duplique el nombre SSID y la configuración de Seguridad de la red inalámbrica (WLAN) en el cliente. En las configuraciones de seguridad del lado del cliente residen la gran mayoría de problemas de conectividad.
4. Asegúrese de que los clientes en las redes inalámbricas (WLAN) localmente cambiadas sean correctamente IP dirigido. Si se utiliza el DHCP, asegúrese de que un servidor por aguas arriba del DHCP esté configurado correctamente y eso proporciona a los direccionamientos a los clientes. Si se utiliza la dirección de los parásitos atmosféricos, asegúrese de que configuren a los clientes correctamente para la subred correcta.
5. Asegúrese de que los puertos UDP 12222 y 12223 estén abiertos en todos los firewalls intermedios.
6. Para resolver problemas más lejos los problemas de la Conectividad del cliente en el puerto de la consola del H-REAP, publique este comando:
   ```
   AP_CLI#show lwapp reap association
   ```
7. Para poner a punto las aplicaciones de la Conectividad del 802.11 un cliente, publique este comando:
   ```
   AP_CLI#debug dot11 state enable
   ```
8. Para poner a punto el proceso de autenticación del 802.1x y los errores de un cliente, publique este comando:
   ```
   AP_CLI#debug dot1x events enable
   ```

Cuentas incorrectas del cliente de los informes inalámbricos del sistema de control (WCS) al AP en el modo H-REAP

Si su entorno de red inalámbrica es manejado por el sistema de control inalámbrico (WCS), este WCS puede señalar a veces a los clientes incorrectos al H-REAP AP, en comparación con las cuentas correctas del cliente especificadas por el regulador.

Este problema es debido al ID de bug CSCsg48059 (clientes registrados de Cisco solamente). El WCS señala las cuentas del cliente que son demasiado altas cuando H-REAP se activa en el regulador. Ésta es la solución alternativa.

1. Para descubrir asocian a cuántos clientes a los APs o al regulador dado, utilice la característica del **monitor > de los clientes WCS**.
2. Busque por el AP o el regulador, que son limitados por el tipo de radio, para evitar los duplicados.
3. Utilice el número total de items encontrados como su número de población verdadero.Usted puede también utilizar el WLC para encontrar la cuenta correcta del cliente.

Este problema se resuelve en la versión inalámbrica 4.0.206.0 del regulador LAN.

Información Relacionada

- Troubleshooting de Punto de Acceso Ligero que no se Une a un Controlador de LAN Inalámbrica
- Guía de Diseño e Implementación de H-Reap
- Configurando el híbrido COSECHE
- Ejemplo de Modos H-REAP de Configuración de Funcionamiento
- Configurando el híbrido COSECHE en el WCS
- Preguntas frecuentes sobre los puntos de acceso ligeros
- Soporte Técnico y Documentación - Cisco Systems