Guía de implementación de REAP en la sucursal

Contenido

Introducción

Este documento proporciona información que debe tenerse en cuenta al implementar el punto de acceso remoto (REAP). Consulte Ejemplo de Configuración de Remote-Edge AP (REAP) con Lightweight APs y Wireless LAN Controllers (WLCs) para obtener información de configuración REAP básica.

Nota: La función REAP se soporta hasta la versión 3.2.215 del WLC. Desde la versión 4.0.155.5 del WLC, esta funcionalidad se denomina Hybrid REAP (H-REAP) con pocas mejoras hasta 7.0.x.x. Desde la versión 7.2.103, esta función se denomina FlexConnect.

Puntos de acceso (AP) basados en el protocolo de punto de acceso ligero (LWAPP) de Cisco tradicionales, (también conocidos como LAP), como los AP 1010, 1020 y 1100 y 1200 Series que ejecutan Cisco IOS® Software Release 12.3(7)JX o posterior, permiten la administración central y

el control a través de Cisco Controladores LAN inalámbricos (WLC) de Cisco. Además, estos LAP permiten a los administradores aprovechar los controladores como puntos únicos de agregación de datos inalámbricos.

Aunque estos LAP permiten a los controladores realizar funciones avanzadas como QoS y aplicación de listas de control de acceso (ACL), el requisito del controlador de ser un único punto de entrada y salida para todo el tráfico de cliente inalámbrico puede dificultar, en lugar de habilitar, la capacidad de satisfacer adecuadamente las necesidades de los usuarios. En algunos entornos, como las oficinas remotas, la finalización de todos los datos de los usuarios en los controladores puede resultar demasiado intensiva en términos de ancho de banda, especialmente cuando hay un rendimiento limitado disponible a través de un enlace WAN. Además, donde los links entre LAP y WLC son propensos a interrupciones, de nuevo comunes con los links WAN a oficinas remotas, el uso de LAP que dependen de WLC para la terminación de datos de usuario conduce a una conectividad inalámbrica cortada durante los tiempos de interrupción de WAN.

En su lugar, puede utilizar una arquitectura AP donde se aprovecha el plano de control tradicional del LWAPP para realizar tareas, como la administración de configuración dinámica, la actualización del software AP y la detección de intrusiones inalámbricas. Esto permite que los datos inalámbricos permanezcan locales, y que la infraestructura inalámbrica se administre de forma centralizada y sea resistente a las interrupciones de la WAN.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

Convenciones

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

Introducción a la arquitectura REAP 1030

El Cisco 1030 REAP separa el plano de control LWAPP del plano de datos inalámbrico para proporcionar funcionalidad remota. Los WLC de Cisco todavía se utilizan para el control y la administración centralizados de la misma manera que los LAPs regulares. La diferencia es que todos los datos del usuario se puentean localmente en el AP. El acceso a los recursos de red locales se mantiene durante las interrupciones de la WAN. La figura 1 ilustra una arquitectura REAP básica.

Figura 1: Diagrama de arquitectura de REAP básico

Nota: Consulte el apéndice A para ver una lista de las diferencias básicas en la funcionalidad de REAP en comparación con los LAP tradicionales.

¿Cuándo se deben utilizar los AP REAP?

El Cisco 1030 REAP AP AP debe utilizarse principalmente en estas dos condiciones:

- Si el link entre el LAP y el WLC es propenso a la interrupción, el REAP 1030 se puede utilizar para permitir a los usuarios inalámbricos acceso ininterrumpido a los datos durante la falla del link.
- Si todos los datos del usuario deben terminarse localmente, lo que significa que en el puerto cableado del AP (en lugar de terminarse en el controlador, ya que los datos son para todos los demás LAP), el REAP 1030 se puede utilizar para permitir el control central a través de la interfaz del controlador y/o el Wireless Control System (WCS). Esto permite que los datos permanezcan locales.

Cuando la cobertura o densidad de usuarios requiere más de dos o tres AP REAP 1030 en un solo sitio, considere la implementación de un WLC 2006 o 2106. Estos controladores pueden soportar hasta 6 LAP de cualquier tipo. Esto puede resultar más viable desde el punto de vista financiero y proporcionar un superconjunto de funciones y funcionalidad en comparación con una implementación de solo REAP.

Al igual que con los AP de la serie 1000, un solo AP 1030 cubre aproximadamente 5000 pies cuadrados. Esto depende de las características de propagación de radiofrecuencia (RF) en cada sitio y del número necesario de usuarios inalámbricos y sus necesidades de rendimiento. En la mayoría de las implementaciones comunes, un solo AP de la serie 1000 puede admitir 12 usuarios a 512 kbps en 802.11b y 12 usuarios a 2 mbps en 802.11a, simultáneamente. Al igual que con todas las tecnologías basadas en 802.11, el acceso a los medios se comparte. Por lo tanto, cuando más usuarios se unen al AP inalámbrico, el rendimiento se comparte en consecuencia. Una vez más, a medida que aumenta la densidad del usuario y/o aumentan los requisitos de rendimiento, considere la adición de un WLC local para ahorrar en costo por usuario y aumentar la funcionalidad.

Nota: Puede configurar los REAP 1030 para que funcionen de manera idéntica a otros LAP. Por lo tanto, cuando se agregan WLC para escalar el tamaño de las infraestructuras WLAN de los sitios remotos, las inversiones REAP existentes pueden seguir siendo aprovechadas.

Implementar REAP

Debido a que el REAP 1030 está diseñado para ubicarse en sitios remotos fuera de la infraestructura del WLC, los LAPs de los métodos tradicionales, sin intervención del usuario, utilizados para detectar y unirse a los controladores (como la opción DHCP 43) generalmente no se utilizan. En cambio, el LAP primero debe ser preparado para permitir que el 1030 se conecte a un WLC nuevamente en un sitio central.

Priming es un proceso en el que los LAPs reciben una lista de WLCs a los que se pueden conectar. Una vez unidos a un único WLC, los LAPs son informados de todos los controladores en el grupo de movilidad y están equipados con toda la información necesaria para unirse a cualquier controlador en el grupo. Consulte Implementación de Cisco 440X Series Wireless LAN Controllers para obtener más información sobre grupos de movilidad, equilibrio de carga y redundancia de controlador.

Para realizar esto en el sitio central, como un centro de operaciones de red (NOC) o un Data Center, los REAP deben estar conectados a la red por cable. Esto les permite detectar un solo WLC. Una vez unido a un controlador, los LAP descargan la versión del LAP OS que corresponde con la infraestructura WLAN. Luego, las direcciones IP de todos los WLC en el grupo de movilidad se transfieren a los AP. Esto permite que los AP, cuando se encienden en sus sitios remotos, descubran y se unan al controlador menos utilizado de sus listas, siempre que la conectividad IP esté disponible.

Nota: La opción DHCP 43 y la búsqueda del Sistema de nombres de dominio (DNS) también funcionan con REAP. Consulte Implementación de Controladores LAN Inalámbricos Cisco 440X Series para obtener información sobre cómo configurar DHCP o DNS en sitios remotos para permitir que los AP encuentren controladores centrales.

En este momento, el 1030 puede recibir direcciones estáticas si lo desea. Esto asegura que el esquema de direccionamiento IP coincida con el sitio remoto de destino. Además, los nombres de WLCs pueden ser ingresados para detallar qué tres controladores cada LAP intentará conectarse. Si estos tres fallan, la funcionalidad automática de balanceo de carga del LWAPP permite al LAP elegir el AP menos cargado de la lista restante de controladores en el clúster. La edición de la configuración del LAP se puede realizar a través de la interfaz de línea de comandos (CLI) o la GUI del WLC, o con mayor facilidad, a través del WCS.

Nota: Los REAP 1030 requieren los WLC a los que se conectan para funcionar en el modo LWAPP de Capa 3. Esto significa que los controladores deben recibir direcciones IP. Además, los WLCs requieren que un servidor DHCP esté disponible en cada sitio remoto, o las direcciones estáticas se deben asignar durante el proceso de inicialización. La funcionalidad DHCP incrustada en los controladores no se puede utilizar para proporcionar direcciones a los LAPs 1030s o a sus usuarios.

Antes de apagar los LAPs 1030 para enviarlos a sitios remotos, asegúrese de que cada 1030 esté configurado en modo REAP. Esto es muy importante porque el valor predeterminado para todos los LAPs es realizar la funcionalidad normal local, y los 1030s deben configurarse para realizar la funcionalidad REAP. Esto se puede hacer en el nivel de LAP a través de la CLI o la GUI del controlador, o con mayor facilidad, a través de las plantillas de WCS.

Funciones básicas de asignación de prioridad REAP

Después de que 1030 REAPs estén conectados a un WLC dentro del grupo de movilidad al que se conectan los REAPs cuando se colocan en sitios remotos, esta información puede ser provista:

Configuración REAP necesaria

- Una lista de direcciones IP para el WLC en el grupo de movilidad (se proporciona automáticamente en la conexión controlador/AP)
- Modo REAP AP AP (los AP deben configurarse para funcionar en modo REAP para realizar

la funcionalidad REAP)

Configuración REAP opcional

- Direcciones IP asignadas estáticamente (una entrada de configuración opcional por AP)
- Nombres WLC primarios, secundarios y terciarios (una entrada de configuración opcional por AP o a través de plantillas WCS)
- Nombre de AP (entrada opcional de configuración informativa por AP)
- Información de ubicación de punto de acceso (entrada opcional de configuración informativa por punto de acceso o a través de plantillas de WCS)

Requisitos de link de REAP a controlador

Cuando planea implementar REAP, es necesario recordar algunos requisitos básicos. Estos requisitos se refieren a la velocidad y latencia de los links WAN que el tráfico de control REAP LWAPP atravesará. El LAP 1030 está diseñado para utilizarse en links WAN, como túnel de seguridad IP, Frame Relay, DSL (no PPPoE) y líneas arrendadas.

Nota: La implementación 1030 REAP LWAPP supone una trayectoria MTU de 1500 bytes entre el AP y el WLC. Cualquier fragmentación que tenga lugar en tránsito debido a una MTU inferior a 1500 bytes produce resultados impredecibles. Por lo tanto, el LAP 1030 no es adecuado para entornos, como PPPoE, donde los routers fragmentan proactivamente paquetes a menos de 1500 bytes.

La latencia de enlaces WAN es particularmente importante porque cada 1030 LAP envía, de forma predeterminada, mensajes de latido a los controladores cada 30 segundos. Después de que se pierden los mensajes del latido, los LAP envían 5 latidos sucesivos, una vez cada segundo. Si ninguno tiene éxito, el LAP determina que la conectividad del controlador se interrumpe y los 1030 vuelven al modo REAP autónomo. Mientras que el LAP 1030 puede tolerar grandes latencias entre sí y el WLC, es necesario asegurar que la latencia no exceda los 100 ms entre el LAP y el controlador. Esto se debe a los temporizadores del lado del cliente que limitan la cantidad de tiempo que los clientes esperan antes de que los temporizadores determinen que una autenticación ha fallado.

Limitaciones de REAP

Aunque el AP 1030 está diseñado para ser administrado centralmente y para proporcionar servicio WLAN durante las interrupciones de link WAN, hay algunas diferencias entre los servicios que el REAP ofrece con conectividad WLC y lo que puede proporcionar cuando la conectividad se interrumpe.

WLAN

Mientras que el REAP 1030 admite hasta 16 WLAN (perfiles inalámbricos que contienen un identificador de conjunto de servicios [SSID] cada uno, junto con todas las políticas de seguridad, QoS y otras), cada uno con su propio ID de conjunto de servicios básicos múltiples (MBSSID), el REAP 1030 sólo puede admitir la primera WLAN cuando se interrumpe la conectividad con un controlador. Durante los tiempos de interrupción del link WAN, todas las WLAN excepto la primera se retiran. Por lo tanto, la WLAN 1 debe estar pensada como la WLAN principal y las políticas de seguridad deben planificarse en consecuencia. La seguridad en esta primera WLAN es

particularmente importante porque si falla el link WAN, también lo hace la autenticación RADIUS backend. Esto se debe a que ese tráfico atraviesa el plano del controlador LWAPP. Por lo tanto, no se concede acceso inalámbrico a ningún usuario.

Se recomienda utilizar un método de autenticación/cifrado local, como la parte de clave previamente compartida del acceso Wi-Fi protegido (WPA-PSK), en esta primera WLAN. La privacidad equivalente a conexión con cables (WEP) es suficiente, pero no se recomienda debido a vulnerabilidades de seguridad conocidas.Cuando se utiliza WPA-PSK (o WEP), los usuarios configurados correctamente pueden obtener acceso a los recursos de red locales incluso si el enlace WAN está inactivo.

Nota: Todos los métodos de seguridad basados en RADIUS requieren que los mensajes de autenticación se transmitan a través del plano de control del LWAPP de vuelta al sitio central. Por lo tanto, todos los servicios basados en RADIUS no están disponibles durante las interrupciones de la WAN. Esto incluye, entre otras, la autenticación MAC basada en RADIUS, 802.1X, WPA, WPA2 y 802.11i.

El REAP 1030 sólo puede residir en una única subred porque no puede realizar el etiquetado de VLAN 802.1q. Por lo tanto, el tráfico en cada SSID termina en la misma subred en la red cableada. Esto significa que, aunque el tráfico inalámbrico se puede segmentar por el aire entre los SSID, el tráfico de usuario no se separa en el lado cableado.

Security

El REAP 1030 puede proporcionar todas las políticas de seguridad de capa 2 compatibles con la arquitectura WAN basada en controlador de Cisco. Esto incluye todos los tipos de cifrado y autenticación de capa 2, como WEP, 802.1X , WPA, WPA2 y 802.11i. Como se indicó anteriormente, la mayoría de estas políticas de seguridad requieren conectividad WLC para la autenticación de backend. WEP y WPA-PSK se implementan por completo en el nivel AP y no requieren autenticación de backend RADIUS. Por lo tanto, incluso si el link WAN no funciona, los usuarios aún pueden conectarse. La función de lista de exclusión de cliente proporcionada en el WLC de Cisco es soportada con el LAP 1030. El filtrado MAC funciona en el 1030 si la conectividad de nuevo al controlador está disponible.

Nota: El REAP no soporta WPA2-PSK cuando el AP está en modo autónomo.

Todas las políticas de seguridad de capa 3 no están disponibles con el LAP 1030. Estas políticas de seguridad incluyen autenticación web, terminación de VPN basada en controlador, ACL y bloqueo de igual a igual, porque se implementan en el controlador. El paso a través de VPN funciona para los clientes que se conectan a concentradores VPN externos. Sin embargo, la función de controlador que permite solamente el tráfico destinado a un concentrador VPN especificado (sólo paso a través de VPN) no lo hace.

traducción de Dirección de Red (NAT)

Los WLC a los que se conectan los REAP no pueden residir detrás de los límites NAT. Sin embargo, los REAP en los sitios remotos pueden sentarse detrás de una caja NAT, siempre que los puertos utilizados para el LWAPP (puertos UDP 12222 y 12223) se reenvíen a los 1030. Esto significa que cada REAP debe tener una dirección estática para que el reenvío de puertos funcione de manera confiable, y que solamente un AP único puede residir detrás de cada instancia NAT. La razón de esto es que solamente puede existir una instancia de reenvío de puerto único por dirección IP NAT, lo que significa que solamente un LAP puede trabajar detrás

de cada servicio NAT en sitios remotos. NAT de uno a uno puede funcionar con varios REAP porque los puertos LWAPP se pueden reenviar para cada dirección IP externa a cada dirección IP interna (dirección IP de REAP estática).

Quality of Service (QoS)

La priorización de paquetes basada en bits de precedencia 802.1p no está disponible porque el REAP no puede realizar el etiquetado 802.1q. Esto significa que no se admiten Wi-Fi Multimedia (WMM) y 802.11e. Se admite la priorización de paquetes basada en SSID y en las redes de bases de identidad. Sin embargo, la asignación de VLAN a través de una red basada en identidad no funciona con el REAP porque no puede realizar el etiquetado 802.1q.

Balanceo de Carga de Clientes y Roaming

En entornos donde hay más de un REAP y donde se espera la movilidad entre AP, cada LAP debe estar en la misma subred. La movilidad de capa 3 no se soporta en el LAP 1030. Por lo general, esto no es una limitación porque las oficinas remotas no suelen emplear suficientes LAP para exigir esa flexibilidad.

El balanceo de carga del cliente agresivo se proporciona a través de todos los REAP en sitios con más de un AP cuando la conectividad del controlador ascendente está disponible (sólo se habilita el balanceo de carga en el controlador del host).

Administración de recursos de radio (RRM)

Cuando hay conectividad con los controladores, 1030 LAPs reciben el canal dinámico y la salida de energía del mecanismo RRM en los WLCs. Cuando el link WAN está inactivo, RRM no funciona y los parámetros de canal y alimentación no se modifican.

Detección no autorizada y funcionalidad de IDS

La arquitectura REAP admite todas las firmas de detección de intrusiones (IDS) y de detección de intrusos que coinciden con las de los LAPs normales. Sin embargo, cuando se pierde la conectividad con un controlador central, no se comparte toda la información recopilada. Por lo tanto, se pierde la visibilidad de los dominios de RF de los sitios remotos.

Resumen de limitación de REAP

La tabla del Apéndice B resume las capacidades del REAP durante el funcionamiento normal y cuando la conexión al WLC a través del link WAN no está disponible.

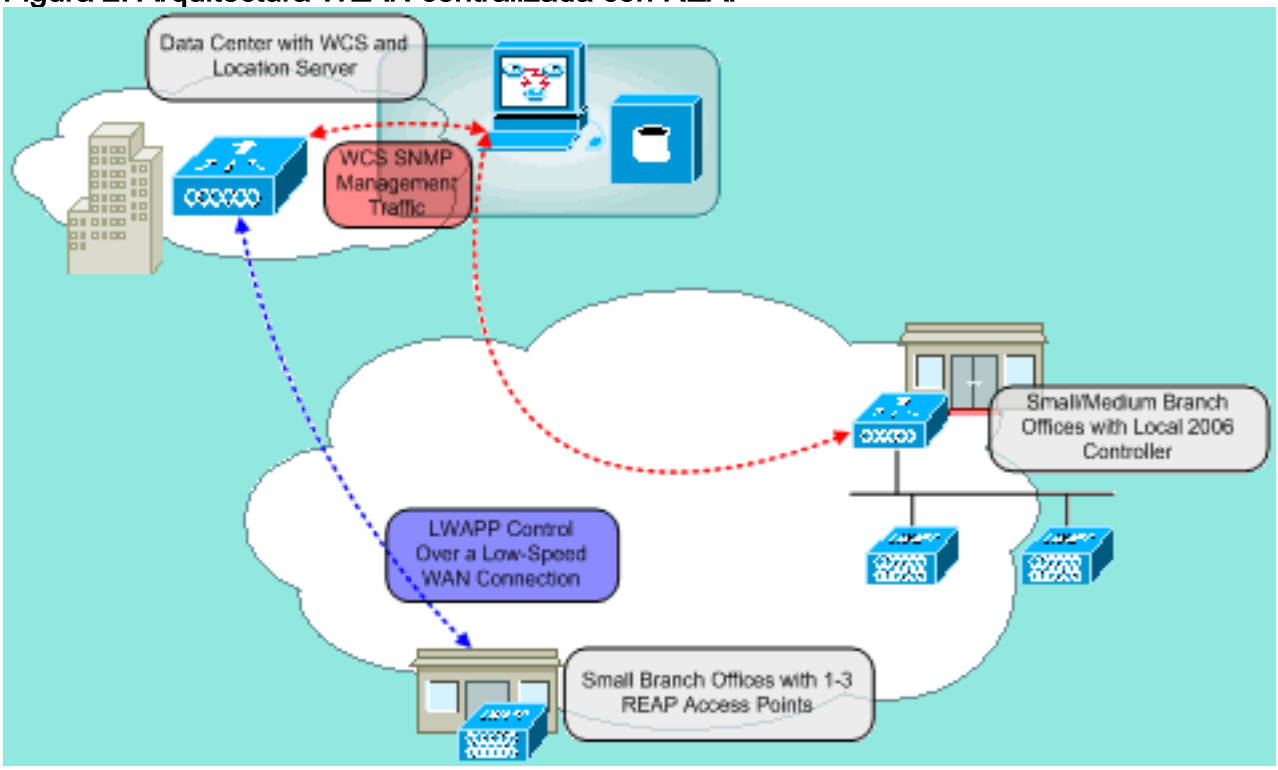
Administración de REAP y arquitectura de WLAN central

La administración 1030 REAP no es diferente a la de los LAPs y WLCs regulares. La administración y la configuración se realizan en el nivel del controlador, ya sea a través de la CLI de cada controlador o de la GUI web. La configuración de todo el sistema y la visibilidad de la red se proporcionan a través de WCS, donde todos los controladores y AP (REAP o de otro modo) se pueden administrar como un único sistema. Cuando se interrumpe la conectividad del controlador REAP, también se interrumpen las capacidades de administración.

Arquitectura WLAN centralizada con REAP

La figura 2 muestra cómo cada parte de la arquitectura LWAPP centralizada funciona en conjunto para satisfacer una variedad de necesidades de red inalámbrica. Los servicios de administración y ubicación se proporcionan de forma centralizada a través de WCS y el dispositivo de ubicación 2700.

Figura 2: Arquitectura WLAN centralizada con REAP



Apéndice A

¿Cuáles son las diferencias principales entre la arquitectura REAP y los LAPs regulares?

- Si la opción DHCP 43 o la resolución DNS no están disponibles en los sitios remotos, el 1030 primero se debe imprimir en la oficina central. Luego, se envía al sitio de destino.
- Cuando falla el link WAN, sólo la primera WLAN permanece activa.Las políticas de seguridad que requieren RADIUS fallarán.Se recomienda la autenticación/cifrado que utiliza WPA-PSK para la WLAN 1. WEP funciona, pero no se recomienda.
- Sin cifrado de capa 3 (solo cifrado de capa 2)
- Los WLC a los que se conectan los REAP no pueden residir detrás de los límites NAT. Sin embargo, los REAP pueden, siempre y cuando cada dirección IP de REAP estática interna tenga ambos puertos LWAPP (12222 y 1223) reenviados a ellos.**Nota:** La traducción de direcciones de puerto (PAT) / NAT con sobrecarga no se admite porque el puerto de origen del tráfico LWAPP que se origina en el LAP puede cambiar con el tiempo. Esto rompe la asociación LWAPP. El mismo problema puede surgir con las implementaciones NAT para REAP donde cambia la dirección del puerto, como PIX/ASA, que depende de la configuración.
- Sólo los mensajes de control LWAPP atraviesan el link WAN.
- El tráfico de datos se puentea en el puerto Ethernet del 1030.
- El LAP 1030 no realiza el etiquetado 802.1Q (VLAN). Por lo tanto, el tráfico inalámbrico de

todos los SSID termina en la misma subred cableada.

Apéndice B

¿Cuáles son las diferencias de funcionalidad entre los modos REAP normal e independiente?

		REAP (modo normal)	REAP (modo independiente)
Protocolos	IPv4	Yes	Yes
	IPv6	Yes	Yes
	Todos los demás protocolos	Sí (solo si el cliente también está habilitado para IP)	Sí (solo si el cliente también está habilitado para IP)
	ARP de proxy IP	No	No
WLAN	Número de SSID	16	1 (el primero)
	Asignación de canal dinámica	Yes	No
	Control de energía dinámico	Yes	No
	Equilibrio de carga dinámico	Yes	No
VLAN	Varias interfaces	No	No
	Compatibilidad con 802.1Q	No	No
Seguridad	Detección de punto	Yes	No

WLAN	de acceso no deseado		
	Lista de exclusión	Yes	Sí (sólo miembros existentes)
	Bloqueo de par a par	No	No
	Sistema de detección de intrusiones	Yes	No
Seguridad de capa 2	autenticación MAC	Yes	No
	802.1X	Yes	No
	WEP (64/128/152 bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	Yes	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Seguridad de capa 3	Autenticación Web	No	No
	IPsec	No	No
	L2TP	No	No
	Paso a través de VPN	No	No
	Listas de control de acceso	No	No

QoS	Perfiles de QoS	Yes	Yes
	QoS de enlace descendente (colas de ordenamiento cíclico ponderado)	Yes	Yes
	Compatibilidad con 802.1p	No	No
	Contratos de ancho de banda por usuario	No	No
	WMM	No	No
	802.11e (futuro)	No	No
	Anulación del perfil AAA QoS	Yes	No
Movilidad	Intra-subred	Yes	Yes
	Intersubred	No	No
DHCP	Servidor DHCP interno	No	No
	Servidor DHCP externo	Yes	Yes
Top	Conexi	No	No

ología	ón directa (2006)		

Información Relacionada

- Ejemplo de Configuración de Remote-Edge AP (REAP) con Lightweight AP y Wireless LAN Controllers (WLC)
- Balanceo de Carga de AP y Reserva de AP en Redes Inalámbricas Unificadas
- Implementación de Cisco 440X Series Cisco 440X Series que despliegan
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems