Guia de implantação do REAP na filial

Contents

Introduction

Este documento fornece informações que precisam ser levadas em consideração ao implantar o Remote-Edge Access Point (REAP). Consulte Exemplo de Configuração de Remote-Edge AP (REAP) com APs Lightweight e Wireless LAN Controllers (WLCs) para obter informações básicas sobre a configuração do REAP.

Observação: o recurso REAP é suportado até o WLC versão 3.2.215. Na versão 4.0.155.5 da WLC, essa funcionalidade é chamada de REAP híbrido (H-REAP) com poucos aprimoramentos até 7.0.x.x. Na versão 7.2.103, esse recurso é chamado de FlexConnect.

Os access points (APs) tradicionais baseados no Cisco Lightweight Access Point Protocol (LWAPP) (também conhecidos como LAPs), como o 1010, 1020 e os APs 1100 e 1200 Series que executam o Cisco IOS® Software Release 12.3(7)JX ou posterior, permitem gerenciamento e

controle centrais por meio dos Wireless LAN Controllers (WLCs) da Cisco. Além disso, esses LAPs permitem que os administradores aproveitem os controladores como pontos únicos de agregação de dados sem fio.

Embora esses LAPs permitam que os controladores executem recursos avançados, como QoS e aplicação da lista de controle de acesso (ACL), a exigência de que o controlador seja um único ponto de entrada e saída para todo o tráfego de clientes sem fio pode impedir, em vez de habilitar, a capacidade de atender adequadamente às necessidades do usuário. Em alguns ambientes, como escritórios remotos, a terminação de todos os dados do usuário nos controladores pode ser muito intensa na largura de banda, especialmente quando o throughput limitado está disponível em um link de WAN. Além disso, onde os enlaces entre LAPs e WLCs são propensos a interrupções, mais uma vez comuns com enlaces WAN para escritórios remotos, o uso de LAPs que dependem de WLCs para terminação de dados do usuário leva à conectividade sem fio interrompida durante períodos de interrupção da WAN.

Em vez disso, você pode utilizar uma arquitetura de AP em que o plano de controle tradicional LWAPP é utilizado para executar tarefas, como gerenciamento de configuração dinâmica, upgrade de software de AP e detecção de intrusão sem fio. Isso permite que os dados sem fio permaneçam locais, e que a infraestrutura sem fio seja gerenciada centralmente e resiliente à interrupção da WAN.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

Introdução à arquitetura do REAP 1030

O Cisco 1030 REAP separa o plano de controle LWAPP do plano de dados sem fio para fornecer funcionalidade remota. As WLCs da Cisco ainda são usadas para controle e gerenciamento centralizados da mesma forma que LAPs regulares. A diferença é que todos os dados do usuário são ligados localmente no AP. O acesso aos recursos da rede local é mantido em todas as interrupções da WAN. A Figura 1 ilustra uma arquitetura REAP básica.

Figura 1: Diagrama de arquitetura do REAP básico

Observação: consulte o Apêndice A para obter uma lista de diferenças básicas na funcionalidade do REAP em comparação com os LAPs tradicionais.

Quando os APs do REAP devem ser usados?

O AP do Cisco 1030 REAP deve ser usado principalmente sob estas duas condições:

- Se o link entre o LAP e a WLC estiver sujeito a interrupções, o REAP 1030 poderá ser usado para permitir aos usuários sem fio acesso ininterrupto aos dados durante falha do link.
- Se todos os dados do usuário precisarem ser terminados localmente, o que significa que na porta com fio do AP (ao contrário de serem terminados no controlador, como os dados são para todos os outros LAPs), o REAP 1030 pode ser usado para permitir o controle central através da interface do controlador e/ou do Wireless Control System (WCS). Isso permite que os dados permaneçam locais.

Quando a cobertura ou a densidade do usuário exigem mais de dois ou três APs 1030 REAP em um único local, considere a implantação de uma WLC 2006 ou 2106. Esses controladores podem suportar até 6 LAPs de qualquer tipo. Isso pode ser financeiramente mais viável e oferecer um superconjunto de recursos e funcionalidades em comparação a uma implantação somente de REAP.

Como acontece com todos os APs 1000 Series, um único AP 1030 cobre aproximadamente 5.000 pés quadrados. Isso depende das características de propagação de radiofrequência (RF) em cada local, bem como do número necessário de usuários sem fio e de suas necessidades de throughput. Na maioria das implantações comuns, um único AP 1000 Series pode suportar 12 usuários a 512 kbps em 802.11b e 12 usuários a 2 mbps em 802.11a, simultaneamente. Como acontece com todas as tecnologias baseadas em 802.11, o acesso à mídia é compartilhado. Portanto, quando mais usuários ingressam no AP sem fio, o throughput é compartilhado de acordo. Novamente, à medida que a densidade do usuário aumenta e/ou os requisitos de throughput aumentam, considere a adição de uma WLC local para economizar no custo por usuário e aumentar a funcionalidade.

Observação: você pode configurar os REAPs 1030 para operar de forma idêntica a outros LAPs. Portanto, quando as WLCs são adicionadas para dimensionar o tamanho da infraestrutura de WLAN de locais remotos, os investimentos existentes em REAP podem continuar a ser aproveitados.

Implantar o REAP

Como o REAP 1030 foi projetado para ser colocado em locais remotos fora da infraestrutura da WLC, os métodos tradicionais de toque zero LAPs usados para descobrir e unir controladores (como a opção de DHCP 43) geralmente não são empregados. Em vez disso, o LAP deve primeiro ser primado para permitir que o 1030 se conecte a uma WLC de volta em um local central.

Primagem é um processo em que os LAPs recebem uma lista de WLCs às quais podem se conectar. Depois de ingressarem em uma única WLC, os LAPs são informados de todos os controladores no grupo de mobilidade e equipados com todas as informações necessárias para ingressar em qualquer controlador no grupo. Consulte Implantação de Cisco 440X Series Wireless LAN Controllers para obter mais informações sobre grupos de mobilidade, balanceamento de carga e redundância de controlador.

Para realizar isso no local central, como um centro de operações de rede (NOC) ou data center, os REAPs devem ser conectados à rede com fio. Isso permite que eles descubram uma única WLC. Depois de ingressarem em um controlador, os LAPs baixam a versão do sistema operacional LAP que corresponde à infraestrutura da WLAN. Em seguida, os endereços IP de todas as WLCs no grupo de mobilidade são transferidos para os APs. Isso permite que os APs, quando ligados em seus locais remotos, descubram e se juntem ao controlador menos utilizado de suas listas, desde que a conectividade IP esteja disponível.

Observação: a opção de DHCP 43 e a pesquisa do Sistema de Nome de Domínio (DNS) também funcionam com REAPs. Consulte Implantação de Cisco 440X Series Wireless LAN Controllers para obter informações sobre como configurar DHCP ou DNS em locais remotos para permitir que os APs localizem controladores centrais.

Nesse momento, os endereços estáticos do 1030 podem ser fornecidos, se desejado. Isso garante que o esquema de endereçamento IP corresponda ao local remoto de destino. Além disso, os nomes das WLCs podem ser inseridos para detalhar quais três controladores cada LAP tentará se conectar. Se esses três falharem, a funcionalidade de balanceamento de carga automático do LWAPP permite que o LAP escolha o AP menos carregado da lista restante de controladores no cluster. A edição da configuração do LAP pode ser feita por meio da interface de linha de comando (CLI) ou GUI da WLC, ou com maior facilidade, por meio do WCS.

Observação: os REAPs 1030 exigem as WLCs às quais se conectam para operar no modo LWAPP da camada 3. Isso significa que os controladores precisam receber endereços IP. Além disso, as WLCs exigem que um servidor DHCP esteja disponível em cada local remoto, ou os endereços estáticos devem ser atribuídos durante o processo de preparação. A funcionalidade DHCP incorporada nos controladores não pode ser usada para fornecer endereços para os LAPs 1030s ou seus usuários.

Antes de desligar os LAPs 1030 para enviar para locais remotos, certifique-se de que cada 1030 esteja definido para o modo REAP. Isso é muito importante porque o padrão para todos os LAPs é executar a funcionalidade local regular e os 1030s precisam ser definidos para executar a funcionalidade REAP. Isso pode ser feito no nível do LAP por meio da CLI ou GUI do controlador, ou com maior facilidade, por meio de modelos WCS.

Funções básicas de impressão do REAP

Depois que 1030 REAPs são conectados a uma WLC dentro do grupo de mobilidade ao qual os REAPs se conectam quando colocados em locais remotos, essas informações podem ser fornecidas:

Configurações necessárias do REAP

- Uma lista de endereços IP para a WLC no grupo de mobilidade (fornecida automaticamente na conexão de controlador/AP)
- Modo de AP REAP (os APs devem ser configurados para operar no modo REAP para

executar a funcionalidade REAP)

Configurações opcionais do REAP

- Endereços IP atribuídos estaticamente (uma configuração opcional de entrada por AP)
- Nomes WLC primários, secundários e terciários (uma configuração opcional de entrada por AP ou por meio de modelos WCS)
- Nome do AP (uma entrada de configuração informativa opcional por AP)
- Informações de localização do AP (uma entrada de configuração informativa opcional por AP ou através de modelos WCS)

Requisitos de link do REAP ao controlador

Quando você planeja implantar REAPs, alguns requisitos básicos precisam ser lembrados. Esses requisitos se referem à velocidade e à latência dos enlaces da WAN que o tráfego de controle do REAP LWAPP atravessará. O LAP 1030 deve ser usado em links WAN, como túnel de segurança IP, Frame Relay, DSL (não PPPoE) e linhas alugadas.

Observação: a implementação LWAPP do 1030 REAP assume um caminho de MTU de 1.500 bytes entre o AP e a WLC. Qualquer fragmentação que ocorra em trânsito devido a um MTU de menos de 1.500 bytes leva a resultados imprevisíveis. Portanto, o LAP 1030 não é adequado para ambientes, como PPPoE, onde os roteadores fragmentam proativamente pacotes para menos de 1500 bytes.

A latência de link de WAN é particularmente importante porque cada LAP 1030 envia, por padrão, mensagens de pulsação aos controladores a cada 30 segundos. Depois que as mensagens de batimento cardíaco são perdidas, os LAPs enviam 5 batimentos cardíacos sucessivos, uma vez a cada segundo. Se nenhuma for bem-sucedida, o LAP determina que a conectividade da controladora seja interrompida e os 1030s revertam para o modo REAP autônomo. Embora o LAP 1030 possa tolerar grandes latências entre ele e a WLC, é necessário garantir que a latência não exceda 100 ms entre o LAP e a controladora. Isso se deve aos temporizadores do lado do cliente que limitam a quantidade de tempo que os clientes aguardam antes que os temporizadores determinem que uma autenticação falhou.

Limitações de REAP

Embora o AP 1030 seja projetado para ser gerenciado centralmente e para fornecer serviço de WLAN durante interrupções de link de WAN, há algumas diferenças entre os serviços que o REAP oferece com conectividade de WLC e o que ele pode fornecer quando a conectividade é interrompida.

WLANs

Embora o REAP 1030 possa suportar até 16 WLANs (perfis sem fio que contêm um SSID (Service Set Identifier, identificador do conjunto de serviços), juntamente com toda a segurança, QoS e outras políticas), cada uma com seu próprio MBSSID (Multiple Basic Service Set ID, ID do conjunto de serviços básicos múltiplos), o REAP 1030 só pode suportar a primeira WLAN quando a conectividade com um controlador é interrompida. Durante os períodos de interrupção do link da WAN, todas as WLANs, exceto a primeira, são desativadas. Portanto, a WLAN 1 deve ser projetada como a WLAN principal e as políticas de segurança devem ser planejadas de acordo. A

segurança nessa primeira WLAN é particularmente importante porque, se o link da WAN falhar, o mesmo acontece com a autenticação RADIUS de backend. Isso ocorre porque esse tráfego atravessa o plano da controladora LWAPP. Portanto, nenhum usuário recebe acesso sem fio.

Recomenda-se que um método de autenticação/criptografia local, como a parte de chave pré-compartilhada do Wi-Fi Protected Access (WPA-PSK), seja usado nesta primeira WLAN. A WEP (Wired Equivalent Privacy) é suficiente, mas não é recomendada devido a vulnerabilidades de segurança conhecidas.Quando a WPA-PSK (ou WEP) é usada, os usuários configurados corretamente ainda podem obter acesso aos recursos da rede local mesmo que o link da WAN esteja inoperante.

Observação: todos os métodos de segurança baseados em RADIUS exigem que as mensagens de autenticação sejam transmitidas através do plano de controle do LWAPP de volta ao local central. Portanto, todos os serviços baseados em RADIUS não estão disponíveis durante interrupções de WAN. Isso inclui, mas não se limita a, autenticação MAC baseada em RADIUS, 802.1X, WPA, WPA2 e 802.11i.

O REAP 1030 só pode residir em uma única sub-rede porque não pode executar a marcação de VLAN 802.1q. Portanto, o tráfego em cada SSID termina na mesma sub-rede na rede com fio. Isso significa que, embora o tráfego sem fio possa ser segmentado no ar entre SSIDs, o tráfego do usuário não é separado no lado com fio.

Security

O REAP 1030 pode fornecer todas as políticas de segurança de Camada 2 suportadas pela arquitetura de WAN baseada em controlador da Cisco. Isso inclui todos os tipos de autenticação e criptografia da camada 2, como WEP, 802.1X, WPA, WPA2 e 802.11i. Como mencionado anteriormente, a maioria dessas políticas de segurança exige conectividade WLC para autenticação de back-end. WEP e WPA-PSK são totalmente implementadas no nível de AP e não exigem autenticação RADIUS de back-end. Portanto, mesmo que o link da WAN esteja inoperante, os usuários ainda podem se conectar. O recurso de lista de exclusão de clientes fornecido no Cisco WLC é suportado com o LAP 1030. A filtragem de MAC funciona no 1030 se a conectividade com o controlador estiver disponível.

Observação: o REAP não suporta WPA2-PSK quando o AP está no modo autônomo.

Todas as políticas de segurança de Camada 3 não estão disponíveis com o LAP 1030. Essas políticas de segurança incluem autenticação da Web, terminação de VPN baseada em controlador, ACLs e bloqueio ponto-a-ponto, pois são implementadas no controlador. A passagem VPN opera para clientes que se conectam a concentradores VPN externos. No entanto, o recurso de controlador que permite somente o tráfego destinado a um VPN Concentrator especificado (somente passagem de VPN) não permite.

Tradução de Endereço de Rede (NAT)

As WLCs às quais os REAPs se conectam não podem residir por trás dos limites de NAT. No entanto, os REAPs em locais remotos podem ficar atrás de uma caixa NAT, desde que as portas usadas para o LWAPP (portas UDP 12222 e 1223) sejam encaminhadas para os anos 30. Isso significa que cada REAP deve ter um endereço estático para que o encaminhamento de portas funcione de forma confiável e que apenas um único AP pode residir atrás de cada instância de NAT. A razão para isso é que apenas uma única instância de encaminhamento de porta pode existir por endereço IP NAT, o que significa que apenas um LAP pode trabalhar por trás de cada

serviço NAT em locais remotos. O NAT um para um pode funcionar com vários REAPs porque as portas do LWAPP podem ser encaminhadas para cada endereço IP externo para cada endereço IP interno (endereço IP do REAP estático).

Quality of Service (QoS)

A priorização de pacotes baseada em bits de precedência 802.1p não está disponível porque o REAP não pode executar a marcação 802.1q. Isso significa que não há suporte para Wi-Fi Multimedia (WMM) e 802.11e. A priorização de pacotes com base no SSID e na rede de bases de identidade é suportada. No entanto, a atribuição de VLAN através da rede baseada em identidade não funciona com o REAP porque não pode executar a marcação 802.1q.

Roaming e balanceamento de carga do cliente

Em ambientes em que há mais de um único REAP e em que a mobilidade entre AP é esperada, cada LAP deve estar na mesma sub-rede. A mobilidade da camada 3 não é suportada no LAP 1030. Normalmente, isso não é uma limitação porque os escritórios remotos geralmente não empregam LAPs suficientes para exigir tal flexibilidade.

O balanceamento de carga agressivo do cliente é fornecido em todos os REAPs em locais com mais de um único AP quando a conectividade do controlador de upstream está disponível (somente o balanceamento de carga está ativado no controlador do host).

RRM (Radio Resource Management, gerenciamento de recursos de rádio)

Quando a conectividade com os controladores está presente, 1030 LAPs recebem saída dinâmica de canal e potência do mecanismo RRM em WLCs. Quando o link da WAN está inativo, o RRM não funciona e as configurações de canal e energia não são alteradas.

Detecção de invasores e funcionalidade IDS

A arquitetura do REAP oferece suporte a todas as IDSs (Detecção de Invasão e Detecção de Intrusão) que correspondem às dos LAPs regulares. No entanto, quando a conectividade é perdida com um controlador central, todas as informações reunidas não são compartilhadas. Portanto, a visibilidade dos domínios de RF de locais remotos é perdida.

Resumo da limitação do REAP

A tabela no Apêndice B resume os recursos do REAP durante a operação normal e quando a conexão com a WLC através do link da WAN não está disponível.

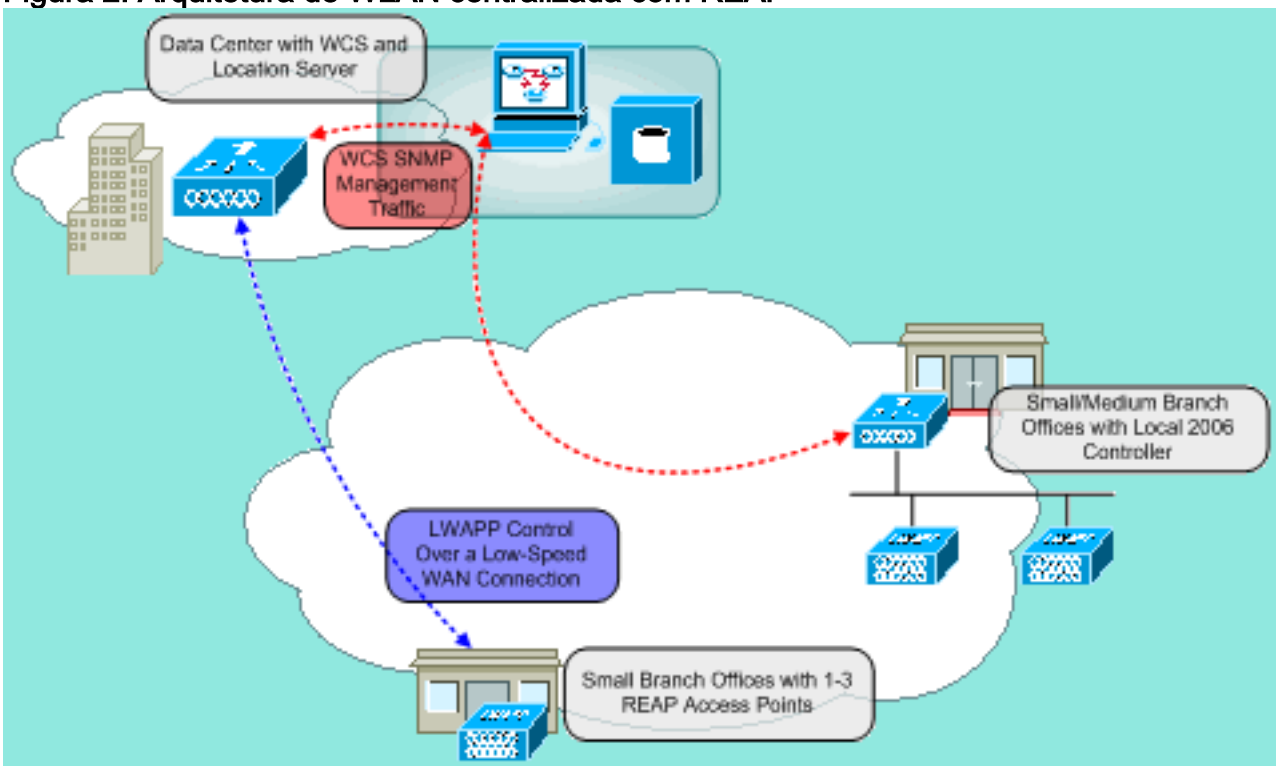
Gerenciar o REAP e a arquitetura de WLAN central

O gerenciamento do REAP 1030 não é diferente do dos LAPs e WLCs regulares. O gerenciamento e a configuração são feitos no nível do controlador, por meio da CLI de cada controlador ou da GUI da Web. A configuração de todo o sistema e a visibilidade da rede são fornecidas através do WCS, onde todos os controladores e APs (REAP ou outros) podem ser gerenciados como um único sistema. Quando a conectividade do controlador REAP é interrompida, os recursos de gerenciamento também são interrompidos.

Arquitetura de WLAN centralizada com REAP

A Figura 2 mostra como cada parte da arquitetura centralizada do LWAPP trabalha em conjunto para atender a uma variedade de necessidades de rede sem fio. Os serviços de gerenciamento e localização são fornecidos centralmente através do WCS e do 2700 Location Appliance.

Figura 2: Arquitetura de WLAN centralizada com REAP



Apêndice A

Quais são as principais diferenças entre a arquitetura do REAP e os LAPs regulares?

- Se a opção de DHCP 43 ou a resolução de DNS não estiver disponível em locais remotos, o 1030 deve primeiro ser inicializado no escritório central. Em seguida, ele é enviado para o local de destino.
- Em caso de falha do link da WAN, apenas a primeira WLAN permanece ativa.As políticas de segurança que exigem RADIUS falharão.A autenticação/criptografia que usa WPA-PSK é recomendada para a WLAN 1. A WEP funciona, mas não é recomendada.
- Sem criptografia de Camada 3 (somente criptografia de Camada 2)
- As WLCs às quais os REAPs se conectam não podem residir por trás dos limites de NAT. No entanto, os REAPs podem, desde que cada endereço IP de REAP estático interno tenha ambas as portas LWAPP (12222 e 12223) encaminhadas a eles.**Observação:** a Conversão de Endereço de Porta (PAT - Port Address Translation) / NAT com sobrecarga não é suportada porque a porta de origem do tráfego LWAPP originado do LAP pode mudar com o tempo. Isso quebra a associação do LWAPP. O mesmo problema pode surgir com implementações de NAT para REAP onde o endereço da porta muda, como PIX/ASA, que depende da configuração.
- Somente as mensagens de controle LWAPP atravessam o link da WAN.
- O tráfego de dados é ligado na porta Ethernet do 1030.
- O LAP 1030 não executa a rotulação 802.1Q (VLANs). Portanto, o tráfego sem fio de todos

os SSIDs termina na mesma sub-rede com fio.

Apêndice B

Quais são as diferenças de funcionalidade entre os modos REAP normal e autônomo?

		REAP (modo normal)	REAP (modo autônomo)
Protocolos	IPv4	Yes	Yes
	IPv6	Yes	Yes
	Todos os outros protocolos	Sim (somente se o cliente também estiver habilitado para IP)	Sim (somente se o cliente também estiver habilitado para IP)
	IP Proxy ARP	No	No
WLAN	Número de SSIDs	16	1 (o primeiro)
	Atribuição dinâmica de canal	Yes	No
	Controle dinâmico de energia	Yes	No
	Balanceamento dinâmico de carga	Yes	No
VLAN	Várias interfaces	No	No
	Suporte 802.1Q	No	No
Segurança WLAN	Detecção de AP invasor	Yes	No
	Lista de	Yes	Sim (somente membros

	exclusões		existentes)
	Bloqueio ponto-a-ponto	No	No
	Sistema de detecção de intrusão	Yes	No
Segurança da camada 2	autenticação 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
Segurança da camada 3	Autenticação da Web	No	No
	IPsec	No	No
	L2TP	No	No
	Passagem de VPN	No	No
	Listas de controle de acesso	No	No
qos	Perfis de QoS	Yes	Yes
	QoS de downli	Yes	Yes

	nk (filas de rodízio ponderadas)		
	Suporte a 802.1p	No	No
	Contratos de largura de banda por usuário	No	No
	WMM	No	No
	802.11e (futuro)	No	No
	Substituição de perfil de QoS AAA	Yes	No
Mobilidade	Intra-sub-rede	Yes	Yes
	Inter-sub-rede	No	No
DHCP	Servidor DHCP interno	No	No
	Servidor DHCP externo	Yes	Yes
Topologia	Conexão direta (2006)	No	No

Informações Relacionadas

- Exemplo de Configuração de Remote-Edge AP (REAP) com APs Lightweight e Controladores

Wireless LAN (WLCs)

- Balanceamento de carga de AP e reversão de AP em redes sem fio unificadas
- Implantação de controladores LAN sem fio do Cisco 440X Series
- Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight
- Suporte Técnico e Documentação - Cisco Systems