COLHA o guia de distribuição no escritório filial

Índice

Introdução

Este documento fornece a informação que precisa de ser tomada na consideração quando você distribui o Access point da Remoto-borda (COLHA). Refira a Remoto-borda AP (COLHA) com AP de pouco peso e controladores do Wireless LAN (WLC) que o exemplo de configuração para básico COLHE a informação de configuração.

Nota: A característica da COLHEITA é apoiada até a liberação 3.2.215 WLC. Do WLC libere 4.0.155.5, esta funcionalidade é chamado Híbrido COLHEITA (H-REAP) com poucos realces até 7.0.x.x. Da liberação 7.2.103, esta característica é chamada FlexConnect.

O protocolo tradicional do Access point da leve Cisco (LWAPP) - os Access point baseados (AP), (igualmente conhecidos como regaços), como os 1010, os 1020, e o 1100 e 1200 Series AP que executa o Software Release 12.3(7)JX ou Mais Recente de Cisco IOS®, permite o

Gerenciamento e o controle centrais através dos controladores do Wireless LAN de Cisco (WLC). Também, estes regaços permitem administradores leverage os controladores como únicos pontos da agregação de dados wireless.

Quando estes regaços permitirem que os controladores executem recursos avançados tais como QoS e aplicação do Access Control List (ACL), a exigência do controlador ser um único ponto do ingresso e da saída para todo o tráfego do cliente Wireless pode impedir, um pouco do que permite, a capacidade para encontrar adequadamente necessidades de usuário. Em alguns ambientes, tais como escritórios remotos, a terminação de todos os dados do usuário em controladores pode provar demasiado a largura de banda intensiva, especialmente quando a taxa de transferência limitada está disponível sobre um link MACILENTO. Também, onde os links entre regaços e WLC são indisponibilidade inclinada, outra vez a terra comum com links MACILENTOS aos escritórios remotos, o uso dos regaços que confiam em WLC para a terminação dos dados do usuário conduz à conectividade Wireless separada durante épocas da interrupção de WAN.

Em lugar de, você pode utilizar uma arquitetura AP onde o plano tradicional do controle LWAPP seja leveraged a fim executar tarefas, tais como o Gerenciamento de configuração dinâmica, upgrade de software AP, e a intrusion detection wireless. Isto permite que os dados wireless permaneçam locais, e o infraestrutura Wireless sejam controlado centralmente e resiliente à interrupção de WAN.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

1030 COLHA a introdução da arquitetura

Cisco 1030 COLHE separa o plano do controle LWAPP do plano wireless dos dados a fim fornecer a funcionalidade remota. Cisco WLC é usado ainda para o controle centralizado e o Gerenciamento da mesma forma como o regular dobra. A diferença é que todos os dados do usuário estão construídos uma ponte sobre localmente no AP. O acesso aos recursos de rede local é mantido durante todo interrupções de WAN. Figura 1 ilustra um básico COLHE a arquitetura.

Figura 1: Básico COLHA o diagrama arquitetónico

Nota: Veja o apêndice A para uma lista de diferenças básicas dentro COLHER a funcionalidade em relação aos regaços tradicionais.

Quando dever COLHER AP para ser usado?

Cisco 1030 COLHE O AP deve ser usado primeiramente sob estas duas circunstâncias:

- Se o link entre o REGAÇO e o WLC é indisponibilidade inclinada, os 1030 REAP podem ser usados para permitir a usuários Wireless o acesso de dados ininterrupto durante a falha do link.
- Se todos os dados do usuário devem ser terminados localmente, que significam na porta prendida do AP (ao contrário da terminação no controlador, porque os dados são para todos regaços restantes), os 1030 REAP podem ser usados para permitir o controle central através da relação do controlador e/ou do sistema de controle wireless (WCS). Isto permite que os dados permaneçam locais.

Onde a cobertura ou a densidade do usuário exigem mais de dois ou três 1030 COLHEM AP em um único local, considere o desenvolvimento de um 2006 ou de 2106 WLC. Estes controladores podem apoiar até os regaços 6 de qualquer tipo. Isto pode provar mais financeiramente viável, e fornece um superset das características e a funcionalidade em comparação com um desenvolvimento da colheita-somente.

Como com todo o 1000 Series AP, tampas únicas 1030 AP aproximadamente 5,000 pés quadrados. Isto depende das características de propagação do Radio Frequency (RF) em cada local, e do número obrigatório de usuários Wireless e de suas necessidades da taxa de transferência. Na maioria de distribuições comum, um único 1000 Series AP pode apoiar 12 usuários em 512kbps em 802.11b e 12 usuários no 2 mbps em 802.11a, simultaneamente. Como com todas as Tecnologias 802.11-based, a mídia de acesso é compartilhada. Consequentemente, quando mais usuários se juntam ao Sem fio AP, a taxa de transferência é compartilhada em conformidade. Além disso, enquanto a densidade do usuário aumenta e/ou os requisitos de throughput aumentam, considere a adição de um WLC local salvar no custo-por-USER e aumentar a funcionalidade.

Nota: Você pode configurar os 1030 colhe para operar-se identicamente a outros regaços. Consequentemente, quando os WLC são adicionados para escalar o tamanho dos infra-estruturos WLAN dos locais remotos, existindo COLHA investimentos pode continuar a ser leveraged.

Distribua COLHEM

Porque os 1030 REAP são projetados ser colocados em locais remotos longe da infraestrutura WLC, os regaços tradicionais, do zero-toque dos métodos usados para descobrir e juntar-se a controladores (tais como a opção de DHCP 43) não são empregados geralmente. Em lugar de, o REGAÇO deve primeiramente ser aprontado a fim permitir que os 1030 conectem a um WLC para trás em uma instalação central.

A escorva é um processo onde os regaços sejam dados uma lista de WLC a que podem conectar. Juntado uma vez a um único WLC, os regaços são informados de todos os controladores no grupo da mobilidade e equipados com toda a informação necessária juntar-se a todo o controlador no grupo. Refira controladores de distribuição do Wireless LAN do Cisco 440X Series para obter mais informações sobre dos Grupos de mobilidade, do Balanceamento de carga, e da redundância de controlador.

A fim executar isto na instalação central, tal como um Network Operations Center (NOC) ou o centro de dados, REAPs deve ser conectada à rede ligada com fio. Isto permite que descubram um único WLC. Juntado uma vez a um controlador, os regaços transferem a versão de OS do REGAÇO que corresponde com o infra-estruturo WLAN. Então, os endereços IP de Um ou Mais Servidores Cisco ICM NT de todos os WLC no grupo da mobilidade são transferidos aos AP. Isto permite os AP, quando posto acima em seus locais remotos, para descobrir e juntar-se a menos controlador utilizado de suas lista, desde que a conectividade IP está disponível.

Nota: O trabalho da opção de DHCP 43 e da consulta do Domain Name System (DNS) com colhe, também. Refira controladores de distribuição do Wireless LAN do Cisco 440X Series para obter informações sobre de como configurar o DHCP ou o DNS em locais remotos a fim permitir que os AP encontrem controladores centrais.

Neste tempo, os 1030 podem ser dados endereços estáticos se desejados. Isto assegura-se de que o esquema de endereçamento de IP combine o local remoto do destino. Também, os nomes WLC podem ser entrados a fim detalhar que três controladores cada REGAÇO tentarão conectar. Se a falha estes três, a funcionalidade de balanceamento de carga automática do LWAPP permite que o REGAÇO escolha o AP menos-carregado da lista restante de controladores no conjunto. A edição da configuração do REGAÇO pode ser feita com o comando line interface(cli) WLC ou o GUI, ou com maior facilidade, com o WCS.

Nota: 1030 REAPs exigem os WLC a que conectam para se operar no modo LWAPP da camada 3. Isto significa que os controladores precisam de ser dados endereços IP de Um ou Mais Servidores Cisco ICM NT. Também, os WLC exigem um servidor DHCP estar disponível em cada local remoto, ou os endereços estáticos devem ser atribuídos durante o processo da escorva. A funcionalidade de DHCP encaixada nos controladores não pode ser usada para fornecer endereços aos regaços 1030s ou aos seus usuários.

Antes que você sem energia os 1030 regaços enviar para fora aos locais remotos, se assegurar de que cada 1030 estejam ajustados PARA COLHER o modo. Isto é muito importante porque todo o padrão para dobra é executar o regular, funcionalidade local, e a necessidade 1030s de ser ajustado para executar COLHEM a funcionalidade. Isto pode ser feito no REGAÇO em nível através do controlador CLI ou GUI, ou com maior facilidade, através dos moldes WCS.

Básico COLHA funções da escorva

Depois de 1030 REAPs é conectada a um WLC dentro do grupo da mobilidade a onde REAPs conecta quando colocada em locais remotos, esta informação pode ser fornecida:

Exigido COLHA ajustes

- Uma lista de endereços IP de Um ou Mais Servidores Cisco ICM NT para o WLC no grupo da mobilidade (fornecido automaticamente em cima da conexão controller/AP)
- COLHA o modo AP (os AP devem ser configurados para se operar dentro COLHEM o modo

a fim executar COLHEM a funcionalidade)

Opcional COLHA ajustes

- Estaticamente endereços IP atribuídos (um ajuste opcional entrado em uma base por-AP)
- Nomes preliminares, secundários, e terciários WLC (um ajuste opcional entrado em uma base por-AP ou através dos moldes WCS)
- Nome AP (um ajuste informativo opcional entrado em uma base por-AP)
- Informação de localização AP (um ajuste informativo opcional entrado em uma base por-AP ou através dos moldes WCS)

Exigências do link do Colher-à-controlador

Quando você planeia distribuir colhe, algumas requisições básico precisam de ser recordados. Estas exigências referem-se à velocidade e a latência dos links MACILENTOS COLHE o tráfego de controle LWAPP atravessará. Os 1030 REGAÇOS são pretendidos ser usados através dos links MACILENTOS, tais como o túnel da Segurança IP, o Frame Relay, o DSL (não PPPoE) e as linhas alugadas.

Nota: Os 1030 COLHEM a aplicação LWAPP supõem um trajeto de 1500 bytes MTU entre o AP e o WLC. Toda a fragmentação que ocorrer no trânsito devido a um byte MTU do sub-1500 conduz aos resultados imprevisíveis. Consequentemente, os 1030 REGAÇOS não são seridos para ambientes, tais como o PPPoE, onde pacotes de fragmento do Roteadores dinamicamente aos bytes do sub-1500.

A latência de link MACILENTO é particularmente importante porque cada 1030 REGAÇOS enviam, à revelia, mensagens ritmada de volta aos controladores cada 30 segundos. Depois que os mensagens ritmada são perdidos, os regaços enviam os heartbeats sucessivos 5, uma vez cada segundo. Se nenhuns são bem sucedidos, o REGAÇO determina que a Conectividade do controlador está separada e os 1030s revertem a autônomo COLHEM o modo. Quando os 1030 REGAÇOS puderem tolerar grandes latências entre se e o WLC, é necessário assegurar-se de que a latência não exceda 100ms entre o REGAÇO e o controlador. Isto é devido aos temporizadores do lado do cliente que limitam a quantidade de tempo dos clientes esperam antes que os temporizadores determinem uma autenticação falharem.

COLHA limitações

Embora os 1030 AP sejam projetados ser controlados centralmente e proporcionar o serviço WLAN durante indisponibilidade MACILENTOS do link, há algumas diferenças entre que serviços a COLHEITA oferece com Conectividade WLC e o que pode fornecer quando a Conectividade é separada.

WLAN

Quando os 1030 REAP puderem apoiar até 16 WLAN (perfis wireless que contêm um [SSID] cada um do Service Set Identifier, junto com toda a Segurança, QoS, e outras políticas), cada um com seu próprio serviço básico múltiplo ID ajustado (MBSSID), os 1030 REAP pode somente apoiar o primeiro WLAN quando a Conectividade com um controlador é interrompida. Durante épocas da indisponibilidade MACILENTO do link, todos os WLAN exceto os primeiros são desarmados. Consequentemente, o WLAN 1 deve ser pretendido como o WLAN e as políticas de

segurança preliminares deve ser planejado em conformidade. A Segurança neste primeiro WLAN é particularmente importante porque se o link MACILENTO falha, faz assim a autenticação RADIUS backend. Isto é porque tal tráfego atravessa o plano do controlador LWAPP. Consequentemente, nenhum usuários é concedido o acesso Wireless.

Recomenda-se que uma autenticação local/método de criptografia, tal como a parcela da chave pré-compartilhada do acesso protegido por wi-fi (WPA-PSK), esteja usada neste primeiro WLAN. O Wired Equivalent Privacy (WEP) basta, mas não é recomendado devido às vulnerabilidades de segurança conhecidas. Quando o WPA-PSK (ou o WEP) são usados, os usuários corretamente configurados podem ainda aceder aos recursos de rede local mesmo se o link MACILENTO está para baixo.

Nota: Todos os métodos de segurança Raio-baseados exigem mensagens de autenticação ser transmitidos através do plano do controle LWAPP de volta à instalação central. Consequentemente, todos os serviços Raio-baseados são não disponíveis durante interrupções de WAN. Isto inclui, mas não é limitado a, autenticação de MAC Raio-baseada, 802.1X, WPA, WPA2, e 802.11i.

Os 1030 REAP podem somente residir em uma sub-rede única porque não pode executar a marcação de VLAN 802.1Q. Consequentemente, o tráfego em cada SSID termina na mesma sub-rede na rede ligada com fio. Isto significa que quando o tráfego Wireless pôde ser segmentado sobre o ar entre SSID, o tráfego de usuário não está separado na face da tela.

Segurança

Os 1030 REAP podem fornecer todas as políticas de segurança da camada 2 apoiadas pela arquitetura MACILENTO controlador-baseada de Cisco. Isto inclui toda a autenticação da camada 2 e tipos das criptografias, tais como o WEP, o 802.1X, o WPA, o WPA2, e o 802.11i. Como indicado previamente, a maioria destas políticas de segurança exigem a Conectividade WLC para a autenticação backend. O WEP e o WPA-PSK são executados inteiramente no AP-nível e não exigem a autenticação RADIUS backend. Consequentemente, mesmo se o link MACILENTO está para baixo, os usuários podem ainda conectar. A característica da lista da exclusão do cliente fornecida em Cisco WLCis apoiado com os 1030 REGAÇOS. Funções de filtragem MAC nos 1030 se a Conectividade de volta ao controlador está disponível.

Nota: REAP não apoia WPA2-PSK quando o AP reage do modo independente.

Todos mergulham 3 políticas de segurança não estão disponíveis com os 1030 REGAÇOS. Estas políticas de segurança incluem a autenticação da Web, a terminação VPN controlador-baseada, os ACL, e a obstrução peer-to-peer, porque são executadas no controlador. O VPN passagem-através de opera-se para os clientes que conectam aos concentradores VPN externos. Contudo, a característica do controlador que permite somente o tráfego destinado para um concentrador VPN especificado (VPN passagem-através de somente) não faz.

Network Address Translation (NAT)

Os WLC a que REAPs conecta não podem residir atrás dos limites NAT. Contudo, colhe em locais de telecontroles pode sentar-se atrás de uma caixa NAT, desde que as portas usadas para LWAPP (portas 12222 e 12223 UDP) são enviadas ao 1030s. Isto significa que cada REAP deve ter um endereço estático para que a porta que envia para trabalhar confiantemente, e que somente um único AP pode residir atrás de cada exemplo NAT. A razão para esta é que somente um exemplo do forwarding da porta única pode existir pelo endereço IP de Um ou Mais

Servidores Cisco ICM NT NAT, que significa que somente um REGAÇO pode trabalhar atrás de cada serviço NAT em locais remotos. O NAT linear pode trabalhar com múltiplo colhe porque as portas LWAPP podem ser enviadas para cada endereço IP externo a cada endereço IP interno (a estática COLHE o endereço IP de Um ou Mais Servidores Cisco ICM NT).

Quality of Service (QoS)

A priorização de pacote baseada nos bit de precedência 802.1p não está disponível porque REAP não pode executar a colocação de etiquetas 802.1q. Isto significa que os multimédios do Wi-fi (WMM) e 802.11e não são apoiados. A priorização de pacote baseada no SSID e os trabalhos em rede das bases da identidade são apoiados. Contudo, a atribuição de VLAN através dos trabalhos em rede Identidade-baseados não trabalha com a COLHEITA porque não pode executar a colocação de etiquetas 802.1q.

Vaguear e função de balanceamento de carga do cliente

Nos ambientes onde mais do que únicos COLHEM esta presente e onde a mobilidade inter-AP é esperada, cada REGAÇO deve estar na mesma sub-rede. A mobilidade da camada 3 não é apoiada nos 1030 REGAÇOS. Tipicamente, esta não é uma limitação porque os escritórios remotos geralmente não empregam bastante regaços para necessitar tal flexibilidade.

O cliente que agressivo o Balanceamento de carga é fornecido através de tudo colhe nos locais com mais do que um único AP quando a Conectividade ascendente do controlador está disponível (é somente o Balanceamento de carga está permitido no controlador do host).

Radio Resource Management (RRM)

Quando a Conectividade aos controladores esta presente, 1030 regaços recebem o canal e saídas de energia dinâmicos do mecanismo RRM nos WLC. Quando o link MACILENTO está para baixo, RRM não funciona, e canaliza e as configurações de energia não são alteradas.

Detecção desonesto e funcionalidade IDS

A arquitetura da COLHEITA apoia toda a assinatura desonesto da detecção e da intrusion detection (IDS) que combinam aquela de regaços regulares. Contudo, quando a Conectividade é perdida com um controlador central, toda a informação recolhida não é compartilhada. Consequentemente, a visibilidade em domínios RF dos locais remotos é perdida.

COLHA o sumário da limitação

A tabela no apêndice B resume as capacidades da COLHEITA durante a operação normal e quando a conexão ao WLC através do link MACILENTO não estiver disponível.

Controle COLHEM e arquitetura de WLAN central

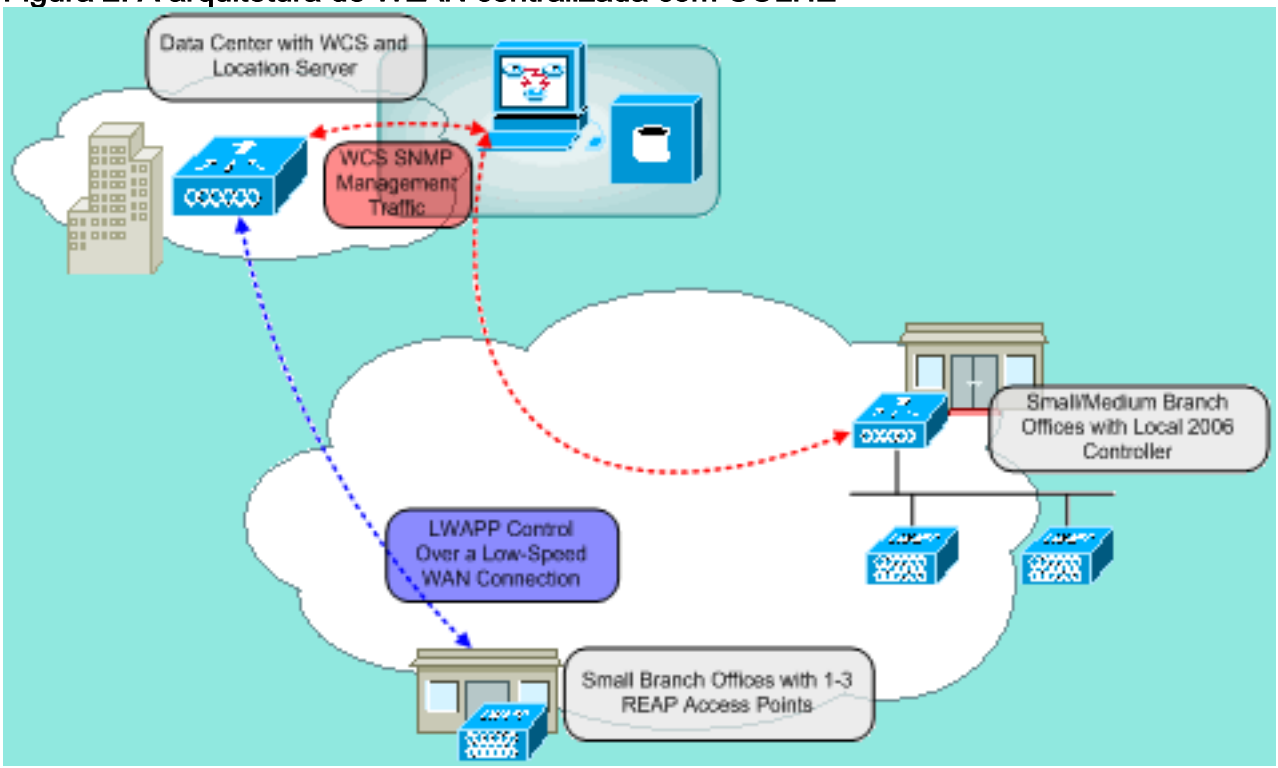
1030 COLHA o Gerenciamento é não diferente do que isso de regaços regulares e de WLC. O Gerenciamento e a configuração são feitos toda no controlador-nível, com o CLI de cada controlador ou Web GUI. A visibilidade da configuração de sistema amplo e da rede é fornecida com o WCS, onde todos os controladores e AP (COLHA ou de outra maneira) podem ser

controlados como um único sistema. Quando a Conectividade do Colher-controlador é interrompida, as potencialidades de gerenciamento estão interrompidas igualmente.

A arquitetura de WLAN centralizada com COLHE

Figura 2 mostra como cada um parte da arquitetura centralizada LWAPP trabalha junto a fim encontrar uma variedade de necessidades da rede de comunicação Wireless. O Gerenciamento e os serviços do lugar são proporcionados centralmente através do WCS e do dispositivo de 2700 lugar.

Figura 2: A arquitetura de WLAN centralizada com COLHE



Apêndice A

Que são as diferenças principal entre a arquitetura da COLHEITA e os regaços do regular?

- Se a opção de DHCP 43 ou a resolução de DNS não estão disponível em locais remotos, os 1030 devem primeiramente ser aprontados no escritório central. Então, é enviado para fora à site de destino.
- Em cima da falha do link MACILENTO, somente o primeiro WLAN permanece ativo.As políticas de segurança que exigem o RAIO falharão.A autenticação/criptografia que usa o WPA-PSK é recomendada para trabalhos WLAN 1. WEP, mas não recomendada.
- Nenhuma criptografia da camada 3 (criptografia da camada 2 somente)
- WLC que REAPs conecta não pode residir atrás dos limites NAT. Contudo, REAPs pode, desde que cada estática interna COLHE o endereço IP de Um ou Mais Servidores Cisco ICM NT tem ambas as portas LWAPP (12222 e 12223) enviadas a elas.**Nota:** A tradução de endereço de porta (PAT) /NAT com sobrecarregamento não é apoiada porque a porta de origem do tráfego LWAPP que origina do REGAÇO pode mudar ao longo do tempo. Isto quebra a associação LWAPP. O mesmo problema pode elevarar com implementações de NAT para REAP onde o endereço de porta muda, como o PIX/ASA pôde, que depende da

configuração.

- Somente as mensagens do controle LWAPP atravessam o link MACILENTO.
- O tráfego de dados é construído uma ponte sobre na porta Ethernet dos 1030.
- Os 1030 REGAÇOS não executam a colocação de etiquetas do 802.1Q (VLAN). Consequentemente, o tráfego Wireless de todos os SSID termina na mesma sub-rede prendida.

Apêndice B

Que são as diferenças em funcionalidade entre o normal e autônomo COLHA modos?

		COLHA (modo normal)	COLHA (modo independente)
Protocolos	IPv4	Sim	Sim
	IPv6	Sim	Sim
	Todos protocolos restantes	Sim (somente se o cliente é igualmente o IP permitido)	Sim (somente se o cliente é igualmente o IP permitido)
	Proxy ARP IP	Não	Não
WLAN	Número de SSID	16	1 (primeiro)
	Atribuição dinâmica do canal	Sim	Não
	Controle de potência dinâmico	Sim	Não
	Balanceamento de carga dinâmico	Sim	Não
VLAN	Interfaces múltiplas	Não	Não
	apoio do 802.1Q	Não	Não
Segurança de	Detecção desonesto AP	Sim	Não

WLAN	Lista da exclusão	Sim	Sim (membros existentes somente)
	Obstrução peer-to-peer	Não	Não
	Sistema de detecção de intrusões	Sim	Não
Segurança da camada 2	Autenticação de MAC	Sim	Não
	802.1X	Sim	Não
	WEP (64/128/152bits)	Sim	Sim
	WPA-PSK	Sim	Sim
	WPA2-PSK	Sim	Não
	WPA-EAP	Sim	Não
	WPA2-EAP	Sim	Não
Segurança da camada 3	Autenticação da Web	Não	Não
	IPsec	Não	Não
	L2TP	Não	Não
	VPN Passagem-através de	Não	Não
	Listas de controle de acesso	Não	Não
qos	Perfis de QoS	Sim	Sim
	Downlink QoS (filas do round robin	Sim	Sim

	pondera do)		
	apoio 802.1p	Não	Não
	Por usuário contrato s da largura de banda	Não	Não
	WMM	Não	Não
	802.11e (futuro)	Não	Não
	Ultrapas sagem do perfil AAA QoS	Sim	Não
Mobi lidad e	Intra-sub-rede	Sim	Sim
	Inter-sub-rede	Não	Não
DHC P	Servidor DHCP interno	Não	Não
	Servidor de DHCP externo	Sim	Sim
Top ologi a	Direct conecta (2006)	Não	Não

Informações Relacionadas

- Remoto-borda AP (COLHA) com AP de pouco peso e exemplo de configuração dos controladores do Wireless LAN (WLC)
- Balanceamento de carga AP e reserva AP em redes Wireless unificadas
- Implantação de Controladoras Wireless LAN Cisco 440X Series
- Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- Suporte Técnico e Documentação - Cisco Systems