Guia de implantação e design do H-Reap

Índice

Introdução

O Access point remoto híbrido da borda (H COLHE) é uma solução Wireless para disposições do escritório filial e do escritório remoto. Isso permite que os clientes configurem e controlem os pontos de acesso em um escritório de filial, ou remoto, a partir de um escritório corporativo através de um link de rede de longa distância (WAN), sem ter que implementar um controlador em cada escritório. O H COLHE Access point pode comutar o tráfego de dados do cliente

localmente e executar a authenticação do cliente localmente quando a conexão ao controlador é perdida. Quando conectado ao controlador, H REAPs pode igualmente tráfego de túnel de volta ao controlador.

Pré-requisitos

Requisitos

REAP híbrida é apoiada somente nos 1040, nos 1130, nos 1140, nos 1240, nos 1250, nos 3500, nos 1260, no AP801, os Access point AP802 e em Cisco WiSM, Cisco 5500, 4400, 2100, 2500, e do 7500 Series do cabo flexível controladores, o interruptor integrado 3750G do controlador do Wireless LAN do catalizador, o módulo de rede do controlador para o Roteadores dos Serviços integrados.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco unificou a versão 7.0 dos controladores
- Controle e abastecimento dos Access point (CAPWAP) 1040 com base nos protocolos, 1130, 1140, 1240,1250, 1260, AP801, AP802 e regaços do 3500 Series

Convenções

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

Fundo das operações CAPWAP

O CAPWAP, em que a arquitetura de rede Wireless unificada de Cisco é baseada, especifica dois modos preliminares diferentes de operação do ponto de acesso Wireless:

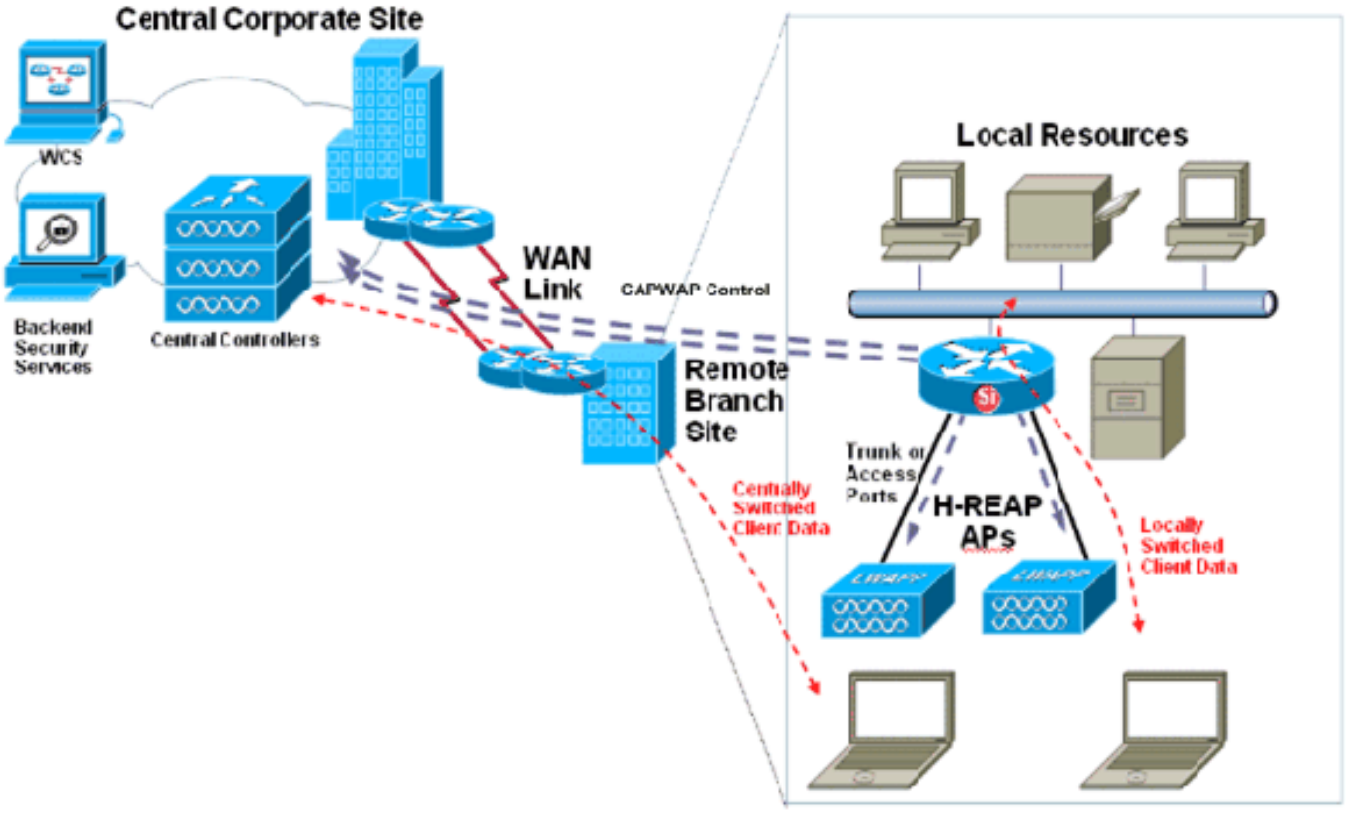
- **Separação-MAC** — No modo Separação-MAC, o sistema compartilha das funções chaves da especificação do 802.11 entre o Access point e o controlador. Em tal configuração, o controlador é não somente responsável para muito do processamento das coisas tais como autenticações do 802.11 e associações, igualmente atua como o único ponto do ingresso e a saída para todo o tráfego de usuário. Túnel que dos Access point Separação-MAC todo o tráfego do cliente ao controlador através de uns dados CAPWAP escava um túnel (o controle CAPWAP igualmente segue o mesmo trajeto.).
- **MAC local** — O MAC local, em executar a funcionalidade completa do 802.11 no Access point, permite a decuplagem do plano dos dados do trajeto do controle terminando todo o tráfego do cliente na porta prendida do Access point. Isto permite não somente o acesso Wireless direto aos recursos locais ao Access point, mas fornece a elasticidade do link permitindo que o trajeto do controle CAPWAP (o link entre o AP e o controlador) esteja para baixo quando o serviço Wireless persistir. Esta funcionalidade é particularmente útil no telecontrole e nos escritórios filiais pequenos através dos links MACILENTOS onde somente um punhado dos Access point é precisado e o custo de um controlador local não é justificado.

Nota: Antes que a liberação 5.2 do controlador, a arquitetura wireless unificada de Cisco estiver baseada no protocolo LWAPP.

O Access point híbrido da Remoto-borda

Controladores do 7500 Series remoto híbrido do Access point, ou H COLHE, é uma característica apoiada por 1040, por 1130, por 1140, por 1240, por 1250, por 3500, por 1260, por AP801, os Access point AP802 e em Cisco WiSM, Cisco 5500, 4400, 2100, 2500, e do cabo flexível da borda, o interruptor integrado 3750G do controlador do Wireless LAN do catalizador, o módulo de rede do controlador para o Roteadores dos Serviços integrados. O H COLHE a característica é apoiado somente a versão de liberação 4.0 do controlador de rede do Cisco Unified Wireless ou em mais atrasado, a característica selecionável deste software permite a fusão de operações da separação e do MAC local CAPWAP para a flexibilidade de distribuição máxima. O tráfego do cliente em H REAPs pode ser comutado localmente no Access point ou ser escavado um túnel de volta a um controlador, que dependa de cada configuração WLAN. Mais, o tráfego localmente comutado do cliente no H REAP pode ser 802.1Q etiquetado a fim prever a separação da face da tela. Durante uma interrupção de WAN, o serviço em tudo comutado localmente, WLAN localmente autenticados persiste.

Este é um diagrama de um H comum COLHE a aplicação:



Enquanto este diagrama indica, H REAP esteve projetado e está pretendido especificamente para disposições do telecontrole e do escritório filial.

Este original esboça o H COLHE a teoria da operação, o controlador e a configuração do ponto de acesso, e as considerações de projeto de rede.

H COLHE a teoria da operação

H COLHE conceitos chaves

Há alguns modos diferentes por que H COLHE a funcionalidade se opera a fim prever interruptor local e central, assim como o survivability MACILENTO do link. A mistura destes dois grupos de modos, ao fornecer uma disposição de funcionalidade, igualmente leva limitações de deferimento segundo o emparelhamento.

Estes são os dois grupos de modos:

- **Central contra o switching local**Os WLAN (séries da Segurança, do QoS, e dos outros parâmetros de configuração amarradas aos SSID) em H REAPs podem ou ser ajustados para exigir todo o tráfego de dados sejam escavados um túnel de volta ao controlador (chamado interruptor central) ou os WLAN podem ser configurados para deixar cair localmente todos os dados do cliente na relação prendida H o REAP (conhecida como o switching local). Os WLAN localmente comutados podem opcionalmente levar o 802.1Q que etiqueta para permitir que tais WLAN sejam segmentados sobre a rede ligada com fio na porta Ethernet do Access point.
- **Conectado contra autônomo**UMA HÍBRIDO-COLHEITA seriam no modo conectado quando seu plano do controle CAPWAP de volta ao controlador é ascendente e operacional, significando que o link MACILENTO não está para baixo. O modo independente está especificado enquanto o estado operacional que o H COLHE entra quando já não tem a Conectividade de volta a seu controlador.

Nota: Todo o H COLHE a autenticação da Segurança que processa (como a derivação backend do [PMK] da autenticação RADIUS e por pares do chave mestre) acontece no controlador quando o Access point estiver no estado conectado. Toda a autenticação do 802.11 e processamento da associação acontecem no H COLHEM, nenhuma matéria em que o modo o Access point está. Quando no modo conectado, H COLHER proxys estas associações/autenticações ao controlador. No modo independente, o Access point não pode informar o controlador de tais eventos.

H COLHE a funcionalidade varia segundo seu modo de operação (se um H REAP reage de conectada ou o modo independente), como cada WLAN é configurado para o interruptor dos dados (central ou local) e a segurança Wireless.

Quando um cliente conecta a um H COLHA o Access point, o Access point encaminha todos os mensagens de autenticação ao controlador e, em cima da autenticação bem sucedida, seus pacotes de dados são comutados então localmente ou escavados um túnel de volta ao controlador, de acordo com a configuração do WLAN a que é conectada. No que diz respeito ao mecanismo de authenticação do cliente e à operação de switching dos dados, os WLAN em H REAP podem estar em qualquer dos seguintes estados segundo a configuração WLAN e o estado da Conectividade do Access point/controlador:

- **autenticação central, interruptor central** — Neste estado, para o WLAN dado, o Access point para a frente todos os pedidos da authenticação do cliente ao controlador e escava um túnel todos os dados do cliente de volta ao controlador, também. Este estado é válido somente quando o trajeto do controle CAPWAP do Access point está acima. Isto significa que o H REAP reage do modo conectado. Todo o WLAN que for escavado um túnel de volta ao controlador é perdido durante a interrupção de WAN, nenhuma matéria o método de autenticação.
- **autenticação central, switching local** — Neste estado, para o WLAN dado, o controlador segura toda a authenticação do cliente, e o H COLHE pacotes de dados do Switches do

Access point localmente. Depois que o cliente autentica com sucesso, o controlador envia um comando de controle CAPWAP ao H REAP que instrui o Access point para comutar que os pacotes de dados do cliente dado localmente. Esta mensagem é enviada pelo cliente em cima da autenticação bem sucedida. Este estado é aplicável somente no modo conectado.

- **autenticação local, switching local** — Neste estado, o H COLHE authenticações do cliente dos punhos do Access point e comuta pacotes de dados do cliente localmente. Este estado é válido somente no modo independente e somente para os tipos do autenticação que podem ser segurados localmente no Access point. Quando um Access point da híbrido-COLHEITA entra o modo independente, a autenticação WLAN que são configurados para aberto, compartilhado, WPA-PSK, ou WPA2-PSK incorporam a `autenticação local,` estado do `switching local` e continuam authenticações do cliente novas.**Nota:** Todos mergulham uma criptografia de dados de 2 Sem fio são segurados sempre no Access point. Todos os processos de authenticação do cliente ocorrem no controlador (ou rio acima do controlador, segundo o WLAN e a configuração de controle) quando o AP estiver no estado conectado.
- **autenticação para baixo, switching local** — Neste estado, para o WLAN dado, o H COLHE rejeições todos os clientes novos que tentarem autenticar, mas continua a enviar balizas e sondar respostas para manter clientes existentes conectados corretamente. Este estado é válido somente no modo independente.Se um WLAN localmente comutado é configurado para qualquer tipo do autenticação que estiver exigido ser processado (ou ao norte de) no controlador (tal como a autenticação de EAP [WEP/WPA/WPA2/802.11i], WebAuth, ou NAC dinâmico), em cima da falha WAN, ele incorpora a autenticação para baixo, estado do switching local. Previamente estaria na autenticação central, estado do switching local. A Conectividade existente do cliente Wireless é mantida e o acesso aos recursos prendidos local persiste, mas nenhuma associação nova é permitida. Se a sessão da web de um usuário cronometra para fora ao usar WebAuth ou, se o intervalo da validez da chave EAP de um usuário expira ao usar o 802.1X, e exige re-fechar, os clientes existentes perdem a Conectividade e estão negados a Conectividade (esta duração é RAIO server-específico e assim, não padronizado). Também, o 802.11 que vagueia eventos (entre H colhe) provoca reautenticações completas do 802.1X e assim, representará o ponto em que a Conectividade é permitida já não aos clientes existentes.Quando a contagem do cliente de tal WLAN iguala zero, o H COLHE cessa todas as funções associadas do 802.11 e já não ilumina-as para o SSID dado, assim movendo o WLAN para o H seguinte COLHA o estado: autenticação para baixo, comutando para baixo.**Nota:** No Software Release 4.2 ou Mais Recente do controlador, os WLAN que são configurados para o 802.1X, o 802.1X WPA, o 802.1X WPA2, ou o CCKM, podem igualmente trabalhar no modo independente. Mas estes tipos do autenticação exigem que um servidor de raio externo esteja configurado. Mais detalhes neste são fornecidos nas seções para vir. Mas, do Software Release 5.1 do controlador, o H COLHE-SE pode ser configurado como um servidor Radius.
- **autenticação para baixo, comutando para baixo** — Neste estado, o WLAN em um H dado COLHE dissocia clientes existentes e para-os de enviar balizas e respostas da ponta de prova. Este estado é válido somente no modo independente.Quando um H COLHE o Access point incorpora o modo independente, ele dissocia todos os clientes que estão em WLAN centralmente comutados. Para a autenticação da Web WLAN, os clientes existentes não são dissociados, mas o H COLHE o Access point já não envia balizas quando o número de clientes associados alcança zero (0). Igualmente envia mensagens da desassociação aos clientes novos que associam à autenticação da Web WLAN. as atividades Controlador-dependentes tais como o controle de acesso de rede (NAC) e a autenticação da Web (acesso do convidado) são desabilitadas, e o Access point não enviam nenhuns relatórios do sistema

de detecção de intrusões (IDS) ao controlador.**Nota:** Se seu controlador é configurado para o NAC, os clientes podem associar somente quando o Access point reage do modo conectado. Quando o NAC é permitido, você precisa de criar (ou quarantined) um VLAN insalubre de modo que o tráfego de dados de todo o cliente que for atribuído às passagens este VLAN através do controlador, mesmo se o WLAN é configurado para o switching local. Depois que um cliente é atribuído a um VLAN quarantined, todos seus pacotes de dados estão comutados centralmente.O Access point da híbrido-COLHEITA mantém a conectividade de cliente mesmo depois que incorpora o modo independente. Contudo, uma vez que o Access point restabelece uma conexão com o controlador, dissocia todos os clientes, aplica a informação de configuração nova do controlador, e a conectividade de cliente dos reallows.

H COLHE o projeto e limitações funcionais

H COLHE considerações MACILENTOS

Porque o H REAP foi projetado especificamente se operar através dos links MACILENTOS, foi aperfeiçoado para tais instalações. Embora H REAP é flexível quando se trata destas encenações do projeto de rede remota, há ainda algumas diretrizes que precisam de ser honradas ao architecting uma rede com o H COLHEM a funcionalidade.

- Um H COLHE o Access point pode ser distribuído com um endereço IP estático ou um endereço de DHCP. No caso do DHCP, um servidor DHCP deve estar disponível localmente e deve poder fornecer o endereço IP de Um ou Mais Servidores Cisco ICM NT para o Access point na inicialização.
- H COLHE apoios até quatro pacotes fragmentados ou um link MACILENTO da unidade de transmissão máxima do 500-byte do mínimo (MTU).
- A latência do Roundtrip não deve exceder 300 milissegundos (Senhora) para dados e Senhora 100 para a Voz e os dados entre o Access point e o controlador, e os pacotes de controle CAPWAP devem ser dados a prioridade sobre todo tráfego restante.
- O controlador pode enviar pacotes de transmissão múltipla sob a forma do unicast ou pacotes de transmissão múltipla ao Access point. Em H COLHA o modo, o Access point pode receber pacotes de transmissão múltipla somente no formulário do unicast.
- A fim usar vaguear rápido CCKM com H COLHA Access point, você precisam de configurar H COLHEM grupos.
- H COLHE o apoio SSID múltiplos dos Access point.
- A integração fora da banda NAC é apoiada somente nos WLAN configurados para H COLHE o interruptor central. Não é apoiada para o uso nos WLAN configurados para H COLHE o switching local.

Nota: Durante uma elevação, cada AP precisa de recuperar uma atualização do código do 4 MB através do link MACILENTO. Elevações do plano e mudança Windows em conformidade.

A fim assegurar-se de que o apoio para esta limitação indicada da latência seja no lugar, recomenda-se fortemente que entre o Access point e o controlador, a prioridade esteja configurada na infraestrutura intermediária para elevar CAPWAP (porta 5246 UDP) à fila a mais prioritária disponível. Sem prioridade colocada no controle CAPWAP, os pontos no outro tráfego de rede podem muito a causa provável H COLHER Access point para deslocar frequentemente do conectado aos modos independentes enquanto o congestionamento de enlace MACILENTO impede que as mensagens do Access point/controlador (e as manutenções de atividade) estejam

entregadas. É altamente recomendado aos projetistas de rede, que planeiam distribuir H COLHEM O AP sobre os links MACILENTOS, para testar todos seus aplicativos.

H frequente COLHE problemas de conectividade sérios das causas do flapping. Sem prioridade da rede adequada no lugar, é prudente colocar controladores em locais remotos para assegurar o acesso Wireless consistente e estável.

Nota: Se H REAP está configurado para escavar um túnel o tráfego do cliente de volta ao controlador ou não, o trajeto de dados CAPWAP é usado para encaminhar todas as pontas de prova do cliente do 802.11 e pedidos da autenticação/associação, mensagens vizinhas RRM, e pedidos EAP e de autenticação da Web de volta ao controlador. Como tal, assegure-se de que os dados CAPWAP (porta 5247 UDP) não estejam obstruídos em qualquer lugar entre o Access point e o controlador.

O híbrido COLHE grupos

A fim organizar e controlar melhor seu H COLHA Access point, você pode criar H COLHE grupos e atribui Access point específicos a eles. Todo o H COLHE Access point em um grupo compartilha do mesmos CCKM, WLAN, e informação de configuração de servidor RADIUS alternativa. Esta característica é útil se você manda H múltiplo COLHER Access point em um escritório remoto ou no assoalho de uma construção e você quer os configurar de uma vez. Por exemplo, você pode configurar um servidor Radius alternativo para um H COLHE o grupo um pouco do que tendo que configurar o mesmo server em cada Access point.

Scalability	Flex 7500	WLC 5500/Wism-2/Wism-1
Total Access Points	2,000	500
Total Clients	20,000	7,000
Max HREAP Groups	500	100
Max APs per HREAP Group	50	25
Max AP Groups	500	500

Os software release 5.0.148.0 do controlador e contêm mais tarde dois que H novo COLHE características do grupo:

- **Servidor Radius alternativo** — Você pode configurar o controlador para permitir um H COLHE o Access point no modo independente para executar a autenticação completa do 802.1X a um servidor Radius alternativo. Você pode configurar um servidor Radius preliminar ou um servidor radius principais e secundários.
- **Autenticação local** — Você pode configurar o controlador para permitir um H COLHE o Access point no modo independente para executar a autenticação RÁPIDA do PULO ou EAP até 20 usuários estaticamente configurados. Com Software Release 5.0 do controlador avante, isto foi aumentado a 100 usuários estaticamente configurados. O controlador envia a

lista estática dos nomes de usuário e senha a cada H COLHE o Access point quando se junta ao controlador. Cada Access point no grupo autentica somente seus próprios clientes associados. Esta característica é ideal para clientes que migra de uma rede autônoma do Access point a um CAPWAP H COLHE a rede do Access point e não a precisa de manter uma grande base de dados de usuário nem de adicionar um outro dispositivo de hardware para substituir a funcionalidade do servidor Radius disponível no Access point autônomo.

Os software release 7.0.116.0 do controlador e contêm mais tarde estes H novo COLHEM características do grupo:

- **Autenticação local** — Esta característica é apoiada agora mesmo quando H COLHE Access point reage do modo conectado.
- **OKC jejuam vagueando** — H COLHE os grupos é exigido para CCKM/OKC que vagueiam rapidamente para trabalhar com H COLHE Access point. Vaguear rápido é conseguido pondo em esconderijo um derivado do chave mestre de uma autenticação de EAP completa de modo que umas trocas de chave simples e seguras possam ocorrer quando um cliente Wireless vagueia a um Access point diferente. Esta característica impede a necessidade de executar uma autenticação de EAP completa do RAIO enquanto o cliente vagueia de um Access point a outro. O H COLHE Access point precisa de obter a informação de cache CCKM/OKC para todos os clientes que puderam associar assim que podem processá-la rapidamente em vez de enviá-la de volta ao controlador. Se, por exemplo, você tem um controlador com 300 Access point e 100 clientes que puderam associar, enviando o esconderijo CCKM/OKC para todos os 100 clientes não são práticos. Se você cria um H COLHA o grupo que compreende um número limitado dos Access point (por exemplo, você cria um grupo para quatro Access point em um escritório remoto), os clientes vagueiam somente entre aqueles quatro Access point, e o esconderijo CCKM/OKC está distribuído entre aqueles quatro Access point somente quando os clientes associam a um deles. Esta característica, junto com o raio e a autenticação local alternativos (Local-EAP), não assegura nenhum tempo ocioso da máquina operacional para suas instalações de filial.

Nota: Vaguear rápido CCKM entre H COLHE e o NON-h COLHE Access point não é apoiado.

Refira configurar Híbrido-COLHEM a seção dos grupos do manual de configuração do controlador de LAN do Cisco Wireless, liberam 7.0 para obter mais informações sobre de como configurar H COLHEM grupos.

Ao tronco ou não ao tronco

H COLHE Access point pode ser conectado aos links do tronco 802.1Q ou aos enlaces de acesso do sem etiqueta. Quando conectado a um enlace de tronco, H COLHE Access point envia seu controle e tráfego de dados CAPWAP de volta ao controlador através do VLAN nativo. Os WLAN localmente comutados podem então ter seu tráfego deixado cair em todos os VLAN disponíveis (nativo, ou de outra maneira). Quando o grupo para operar sobre um enlace de acesso (sem a visibilidade do 802.1Q), H colher dianteiro todas as mensagens CAPWAP e dados do usuário para fora localmente comutados ao único, a sub-rede do sem etiqueta a que está conectado.

As diretrizes gerais para a seleção do modo do switchport para H REAPs são como segue:

- Use um enlace de tronco se mais de um WLAN está configurado para o switching local e se o tráfego nestes SSID precisa de ser deixado cair em sub-redes diferentes. O Access point e o switchport ascendente precisam de ser configurados para o entroncamento do 802.1Q. A

configuração de H colhe para o entroncamento do 802.1Q é a maioria de configuração comum e fornece a maioria de flexibilidade. O VLAN nativo igualmente precisa de ser configurado no switchport que o H REAP está conectado como a toda a comunicação CAPWAP entre o AP e o WLC está no VLAN nativo.
- Use um enlace de acesso quando H colhe não tem mais do que um único WLAN localmente comutado nem tem o múltiplo WLAN localmente comutados que não exigem a separação do prender-lado. Esteja ciente que um enlace de tronco pode ainda ser desejável sob estas condições se a separação entre a Mensagem CAPWAP e os dados do usuário é desejada. Mas, este é nem um requisito de configuração, nem um risco de segurança.

Nota: H COLHE Access point opta para operar sobre o sem etiqueta, relações do enlace de acesso.

H COLHE a descoberta do controlador

H COLHE apoios cada mecanismo de descoberta do controlador característico dos Access point na arquitetura de rede Wireless unificada de Cisco. Uma vez que o Access point tem um endereço IP de Um ou Mais Servidores Cisco ICM NT (fornecido dinamicamente através do DHCP, ou com o endereçamento estático) tenta descobrir controladores no sistema através da transmissão IP, a opção de DHCP 43, DNS, e sobre - areje o abastecimento (OTAP). Finalmente, H REAPs recorda os endereços IP de Um ou Mais Servidores Cisco ICM NT do controlador a que foram conectados previamente. Refira o registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (WLC) para obter informações sobre dos métodos diferentes que um REGAÇO pode usar para se registrar com um WLC.

Há algumas advertências a manter-se na mente com respeito à descoberta do controlador. Estas considerações aplicam-se a todos os pontos de acesso Aironet e não apenas H colhe.

- A opção de DHCP 43 é somente um mecanismo de descoberta viável para H COLHE se o Access point recebe seu endereçamento de IP com o DHCP.
- O OTAP trabalha somente para os pontos de acesso Aironet que têm conectado já a um controlador e a um código transferido. Enviam sem firmware de rádio, assim que o OTAP não trabalha diretamente fora da caixa. O OTAP igualmente exige que outros Access point próximos encontraram e conectaram a um controlador em que o OTAP é permitido. Esta característica é Obsoleto da liberação WLC 6.0 avante.
- Um Access point em que H COLHE a funcionalidade é apoiado não apoia o modo da camada 2 LWAPP CAPWAP. Os controladores devem ser ajustados para operar-se com camada 3 LWAPP CAPWAP.
- Refira controladores de distribuição do Wireless LAN do Cisco 440X Series para obter mais informações sobre da descoberta do Access point/controlador. operações

Além destes mecanismos de descoberta tradicionais do controlador, o Software Release 4.0 e Mais Recente permite que os pontos de acesso Aironet com portas de Console apoiem agora o abastecimento manual através do console CLI. Os Access point podem agora manualmente ser configurados para o endereçamento do IP Estático, a atribuição do hostname, e os endereços IP de Um ou Mais Servidores Cisco ICM NT dos controladores a que os Access point devem conectar. Isto significa que nos locais onde outros mecanismos de descoberta não estão disponíveis, os Access point podem ser configurados com toda a configuração da conectividade necessária manualmente através da porta de Console.

Embora esta característica seja apoiada em cada ponto de acesso Aironet com uma porta de Console, não apenas aquelas configuradas para H COLHEM, esta funcionalidade é

particularmente útil para H colhe porque são mais prováveis se encontrar instalados nos locais que não são equipados com os servidores DHCP e os mecanismos de descoberta do controlador, tais como dentro um escritório filial. Como tal, este acesso de console novo previne a necessidade de enviar H colhe duas vezes: uma vez a uma instalação central pelo abastecimento e uma segunda vez ao local remoto para a instalação.

H COLHE características suportadas

Porque H COLHE os Access point são projetados ser colocados através dos links MACILENTOS dos controladores, estão não somente lá as considerações de projeto que precisam de ser mantidas na mente ao architecting uma rede Wireless com H colhe, mas há igualmente algumas características que são completamente ou em-parte unsupported.

Não há nenhuma limitação do desenvolvimento no número de H COLHE Access point para cada lugar.

H COLHE a matriz de recurso

Refira H COLHEM a matriz de recurso para obter mais informações sobre das características apoiadas com H COLHEM.

Recursos de segurança apoiados

O apoio da Segurança no H COLHE varia, que depende dos modos e dos estados mencionados previamente. Qualquer tipo da Segurança que exigir o controle sobre o trajeto de dados tal como o VPN, não trabalha com tráfego em WLAN localmente comutados porque o controlador não pode exercitar o controle sobre os dados que não são escavados um túnel de volta a ele. Qualquer outro tipo trabalhos da Segurança WLAN em centralmente ou localmente comutados, desde que o trajeto entre o H COLHE e o controlador está acima. Quando esta conduíte estiver para baixo, simplesmente um subconjunto destas opções de segurança permite que os clientes novos conectem aos WLAN localmente comutados.

Como mencionado previamente, a fim apoiar a autenticação de EAP do 802.1X, H COLHE Access point na necessidade do modo independente de ter seus próprios servidores Radius para autenticar clientes. Este servidor Radius alternativo pode ser esse usado pelo controlador. Você pode configurar um servidor Radius alternativo para H individual COLHE Access point através do controlador CLI ou para H COLHE grupos com o GUI ou o CLI. Um servidor de backup configurado para um ponto de acesso individual cancela a configuração de servidor RADIUS para um H COLHE o grupo.

Vaguear seguro rápido do apoio da versão 4.2.61.0 e mais recente WLC com Cisco centralizou o gerenciamento chave (CCKM). H COLHE vaguear seguro da camada 2 dos apoios do modo rapidamente com CCKM. Esta característica impede a necessidade para a autenticação de EAP completa do RAIO enquanto o cliente vagueia de um Access point a outro. A fim usar vaguear rápido CCKM com H COLHA Access point, você precisam de configurar H COLHEM grupos. O CCKM trabalha no modo independente para já clientes conectados mas não para clientes novos.

Refira configurar Híbrido-COLHEM a seção dos grupos do manual de configuração do controlador de LAN do Cisco Wireless, liberam 7.0 para obter mais informações sobre de como configurar H COLHEM grupos.

Com H COLHA no modo conectado, o controlador está livre impor a exclusão do cliente/pôr a fim impedir que alguns clientes associem a seus Access point. Esta função pode acontecer na forma automatizada ou manual. De acordo com global e as configurações por-WLAN, os clientes podem ser excluídos para um host das razões, que varie das tentativas repetidas da autenticação falha ao roubo IP, e para qualquer dada quantia de tempo. Os clientes podem igualmente ser inscritos nesta lista da exclusão manualmente. O exercício desta característica é somente possível quando o Access point reagir do modo conectado. Mas, os clientes que foram colocados nesta lista da exclusão permanecem incapazes de conectar ao Access point, mesmo quando reagir do modo independente.

Nota: Os WLAN que usam a autenticação de MAC (local ou rio acima) são já não permitem as authenticações do cliente adicionais quando o Access point reage do modo independente, idênticas à maneira um WLAN similarmente configurado com 802.1X ou WebAuth operar-se-ia no mesmo modo.

Apoio da autenticação da Web

A autenticação do web interna, hospedada no controlador do Wireless LAN, é apoiada para os WLAN que são comutados centralmente ou localmente. Contudo, a autenticação do web externa é apoiada somente em um WLAN centralmente comutado.

Nota: Nenhum método de autenticação da Web é apoiado quando um H REAP reagir do modo independente.

Características da infraestrutura apoiadas

RRM

Devido ao fato de que muitas disposições remotas têm somente um punhado pequeno de H colhe, funcionalidade completa do Radio Resource Management (RRM) não pôde ser apoiado em cada H COLHE o local. O código completo RRM esta presente em H COLHE, mas os algoritmos do controle de potência de transmissão (TPC) em RRM não são provocados até quatro ou mais Access point esteja dentro da escala de se. Assim, algum H COLHE as instalações pôde nunca pôr seus rádios para baixo. Como tal, sem nunca poder pôr para baixo seus rádios no primeiro lugar, H REAPs não ajusta a potência de transmissão compensar para cima no caso de uma detecção do furo da cobertura.

No modo independente, as funções RRM em H colhem que exigem o controlador que processar não é suportado.

Refira a gerência de recursos de rádio sob redes Wireless unificadas para mais informação e detalhes operacionais de RRM.

DF

A seleção dinâmica da frequência (DF) é apoiada no conectado e modos independentes.

Seguimento do lugar

A capacidade para prever a determinação exata do lugar do dispositivo varia extremamente do lugar ao lugar, baseado extremamente no número, densidade, e a colocação de H colhe. A precisão do lugar articula-se pesadamente na riqueza da coleção de informação do sinal do

dispositivo, que correlaciona diretamente com o número de ponto de acesso que pode ouvir um dispositivo dado. Porque H COLHE disposições varia no espaço, esta informação de localização pode extremamente ser reduzida e assim a precisão do lugar pôde sofrer em conformidade. Quando H COLHER as disposições tentam indicar o lugar dos dispositivos com a confiança a mais alta possível, reivindicações indicadas da precisão do lugar de Cisco não estão apoiadas em tais ambientes.

Nota: H REAP não foi projetado proporcionar serviços do lugar. Consequentemente, Cisco não pode apoiar indicou que reivindicações da precisão do lugar em H COLHE disposições.

Mobilidade L2 e L3

A camada regular 2 que vagueia é apoiada para WLAN localmente comutados. A fim prever tal vaguear, assegure-se de que os VLAN atribuídos aos WLAN localmente comutados estejam consistentes através de todo o H colham no meio, que vaguear é exigido. Isto significa que os clientes não estão exigidos ao re-DHCP em cima dos eventos vagueando. Isto ajuda a diminuir as latências associadas com o tais vagueia.

Vaguear eventos entre H colhe nos WLAN localmente comutados pode tomar entre a Senhora dos 50 pés e a Senhora 1500, que dependem da latência MACILENTO, dos projetos RF e das características ambientais, assim como a Segurança datilografa e aplicações vagueando cliente-específicas.

A camada 3 que vagueia não é apoiada para WLAN localmente comutados, mas é apoiada para WLAN centralmente comutados.

NAT/PAT

O NAT e a PANCADINHA não são apoiados para H COLHEM Access point.

O outro H COLHE limitações

- H REAPs não apoia o WGB.
- Se você configurou um WLAN localmente comutado, a seguir o Access Control Lists (ACLs) não trabalha e não está apoiado. Em um WLAN centralmente comutado, os ACL são apoiados.
- Todas as mudanças a uma configuração localmente comutada WLAN na causa do controlador uma perda temporária na Conectividade como a configuração nova são aplicadas ao H COLHEM. Como tal, todos os clientes nestes WLAN localmente comutado obtêm temporariamente desligado. O WLAN é permitido imediatamente e os clientes reassociam para trás.
- O controlador pode enviar pacotes de transmissão múltipla sob a forma do unicast ou pacotes de transmissão múltipla ao Access point. Em híbrido-COLHA o modo, o Access point pode receber pacotes de transmissão múltipla somente no formulário do unicast.

Nota: Se o H REAP está conectado ao link do tronco 802.1Q e há localmente os WLAN comutados configurados para o VLAN, a seguir a ordem da configuração WLAN transforma-se importante devido a uma limitação no projeto. Se você muda a ordem do WLAN por exemplo o WLAN 1 está configurado para o ssid `WLAN-um` e WLAN 2 está configurado para o ssid `WLAN-b` e sua ordem é mudada com a configuração WLAN 1 transforma-se o ssid `WLAN-b` e WLAN 2 transforma-se o ssid `WLAN-um`, a seguir ambos os WLAN perdem seu mapeamento VLAN que é configurado do WLC.

Nota: A mesma edição aplica-se de um H COLHE que se junte a um controlador diferente que tenha a ordem diferente dos mesmos WLAN. Os controladores principais e secundários para um híbrido COLHEM o Access point devem ter a mesma configuração. Se não, o Access point pode perder sua configuração, e determinadas características, tais como a ultrapassagem WLAN, o grupo VLAN AP, número de canal estático, e assim por diante, não podem potencialmente operar-se corretamente. Além, certifique-se duplicar o SSID do H COLHEM o Access point e o seu número do índice em ambos os controladores.

Tolerância a falhas

H COLHE a tolerância de defeito permite que o acesso Wireless e os serviços ramifiquem clientes quando:

- H COLHE o ramo AP perde a Conectividade com o controlador principal.
- H COLHE o ramo AP está comutando ao controlador secundário.
- H COLHE o ramo AP está restabelecendo a conexão ao controlador principal.

H COLHE a tolerância de defeito, junto com o EAP local como esboçado acima, forneça junto o tempo ocioso da máquina zero do ramo durante uma parada de rede. Esta característica é permitida à revelia e não pode ser desabilitada. Não exige nenhuma configuração no controlador ou no AP. Contudo, assegurar lisamente trabalhos da tolerância de defeito e é aplicável, este critérios deve ser mantido:

- Pedir e configurações WLAN têm que ser idênticos através dos controladores principais e de backup.
- O mapeamento VLAN tem que ser idêntico através dos controladores principais e de backup.
- O Domain Name da mobilidade tem que ser idêntico através dos controladores principais e de backup.
- Recomenda-se usar a plataforma do controlador como ambos os controladores principais e de backup.

Resumo

- H REAP não desligará clientes quando o AP não está conectando de volta ao mesmo controlador fornecido lá é nenhuma mudança na configuração no controlador.
- H REAP não desligará clientes quando conectar ao controlador de backup fornecido lá não é nenhuma mudança na configuração e o controlador de backup é idêntico ao controlador principal.
- H REAP não restaurará seus rádios na conexão de volta ao controlador principal fornecido lá é nenhuma mudança na configuração no controlador.

Limitações

- Apoiado somente para H COLHA com central/autenticação local com switching local.
- Os clientes centralmente autenticados exigem a reautenticação completa se o temporizador da sessão cliente expira antes que o H COLHA o Switches AP de autônomo ao modo conectado.
- Os controladores principais e de backup devem estar no mesmo domínio da mobilidade.

H COLHE a configuração

Preparação da rede ligada com fio

A primeira etapa a distribuir um H COLHE a rede é configurar o interruptor a que o H REAP conectará. Esta configuração de switch do exemplo inclui uma configuração de VLAN nativa (a sub-rede em que H REAPs se comunicará com o controlador com CAPWAP) e duas sub-redes em que os dados dos clientes de dois WLAN localmente comutados terminarão. Se o endereçamento de IP não está fornecido aos Access point e aos clientes de WLAN localmente comutados através do interruptor ascendente (como mostrado abaixo), a seguir ou os serviços DHCP precisam de ser proporcionados através dos outros meios, ou o endereçamento precisa de ser fornecido estaticamente. Embora o DHCP seja recomendado, alguns provavelmente optarão ao endereçamento do ponto de acesso estático e fornecerão endereços dos usuários Wireless através do DHCP. As configurações de switch supérfluas foram removidas deste exemplo para simplificar.

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99

ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

Nota: O endereçamento de IP real neste exemplo e em todas as configurações subsequente é puramente para fins ilustrativos. Como tal, o endereçamento de IP DEVE ser planejado com cada rede individual e necessidade na mente.

Neste exemplo de configuração, o H REAP é conectado à primeira interface fastethernet e recebe o endereçamento de IP através do DHCP do interruptor no VLAN nativo (VLAN10). Os vlan desnecessária são podados do enlace de tronco conectado ao H COLHEM a fim limitar o processamento de pacotes estranhos. Os VLAN 11 e 12 foram preparados para fornecer o endereçamento de IP aos clientes dos dois WLAN que lhes são amarrados.

Nota: O interruptor a que H REAPs conecta a Conectividade ascendente das necessidades à infraestrutura de roteamento. H COLHE a ordem dos melhores prática que a infraestrutura de

roteamento remote-site/WAN dá a prioridade ao controle CAPWAP (porta 5246 UDP).

Está aqui uma configuração de exemplo de um roteador fluxo acima onde o H COLHA O AP seja conectado a fim dar a prioridade ao tráfego CAPWAP.

```
ip cef
!
frame-relay switching
!
class-map match-all 1
  match access-group 199
!
policy-map mypolicy
  class 1
   bandwidth 256
!
interface Serial0/0
ip address 10.1.0.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 101
frame-relay intf-type dce
service-policy output mypolicy
!
access  list  199  permit  udp  any  any  eq  5246
```

Descoberta do controlador H-REAP usando comandos CLI

H REAPs descobrirá o mais geralmente controladores ascendentes através da opção de DHCP 43 ou da resolução de DNS. Sem o qualquer um destes métodos disponíveis, pode ser desejável fornecer instruções detalhadas aos administradores em locais remotos de modo que cada H REAP possa ser configurado com o endereço IP de Um ou Mais Servidores Cisco ICM NT dos controladores a que devem conectar. Opcionalmente, H COLHE o endereçamento de IP pode ser ajustado manualmente também (se o DHCP é não disponível ou não desejado).

Detalhes deste exemplo como o endereço IP de Um ou Mais Servidores Cisco ICM NT H um REAP, o hostname, e o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador podem ser ajustados através da porta de Console do Access point.

```
AP_CLI#capwap ap hostname ap1130
ap1130#capwap ap ip address 10.10.10.51 255.255.255.0
ap1130#capwap ap ip default-gateway 10.10.10.1
ap1130#capwap ap controller ip address 172.17.2.172
```

Nota: Os Access point devem executar o Cisco IOS Software Release 12.3(11)JX1 ou Mais Recente LWAPP-permitido da imagem de recuperação IOS® a fim apoiar estes comandos CLI fora da caixa. Os Access point com o prefixo de SKU do REGAÇO (por exemplo, AIR-LAP-1131AG-A-K9), enviado sobre ou depois de junho 13, 2006 executam o Cisco IOS Software Release 12.3(11)JX1 ou Mais Recente. Estes comandos estão disponíveis a algum Access point que enviar do fabricante que executa este nível de código, tiver o código promovido manualmente a este nível, ou é promovido automaticamente conectando a uma versão 6.0 ou mais recente running do controlador.

Estes comandos configuration são aceitados somente quando o Access point reage do modo independente.

Quando um Access point foi conectado nunca a um controlador antes, os Access point têm a senha do padrão CLI de Cisco. Uma vez que os Access point são conectados a um controlador, nenhuma configuração de CLI pode ser feita através do console do Access point até que a senha esteja mudada. Este comando CLI-somente é incorporado no controlador com esta sintaxe:

```
(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
```

Para o Access point acima, este comando pôde ser usado:

```
(WLC_CLI)>config ap username admin password pass ap1130
```

Nota: Embora este comando exija a criação de um username, este campo não é executado e é reservado presentemente para uso futuro.

Nota: Todos os **comandos show and debug** se operarão muito bem sem as senhas padrão do Access point que estão sendo mudadas.

Configuração de controle H-REAP

Uma vez que o H REAP descobriu e se juntou ao controlador, todo o H COLHE configurações está feito através da Web ou das interfaces de linha de comando do controlador (alternativamente, a configuração pode ser feita centralmente com o [WCS] wireless do sistema de controle). O H COLHE configurações nesta seção é executado através da interface gráfica do controlador.

Comece criando e configurando os WLAN desejados. Para este exemplo de configuração, os WLAN são como segue (*configurações do alfaiate como necessário*):

WLAN SSID	Security	Comutação
Corporativo	WPA2 (802.1X)	Local
RemoteSite	WPA2 - PSK	Local
Convidado	WebAuth	Central

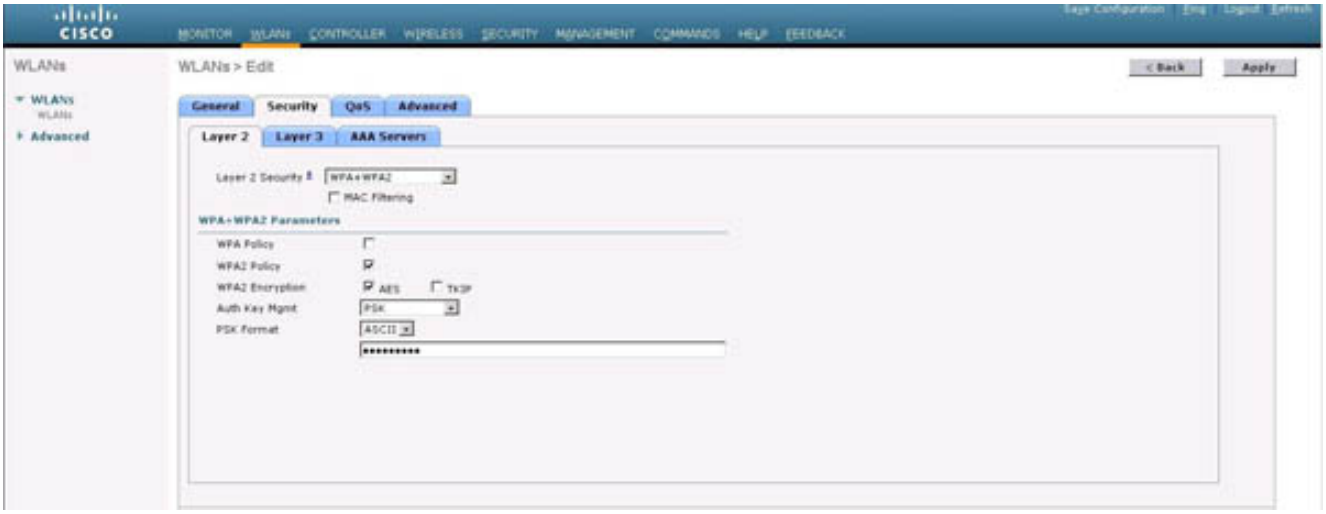
Para que um H COLHA o Access point para operar-se como um H COLHE, o controlador a que está conectado deve ter pelo menos um WLAN localmente comutado (sem isto, requisito de alta disponibilidade da funcionalidade H REAP não será realizado).

Termine estas etapas a fim configurar um WLAN localmente comutado:

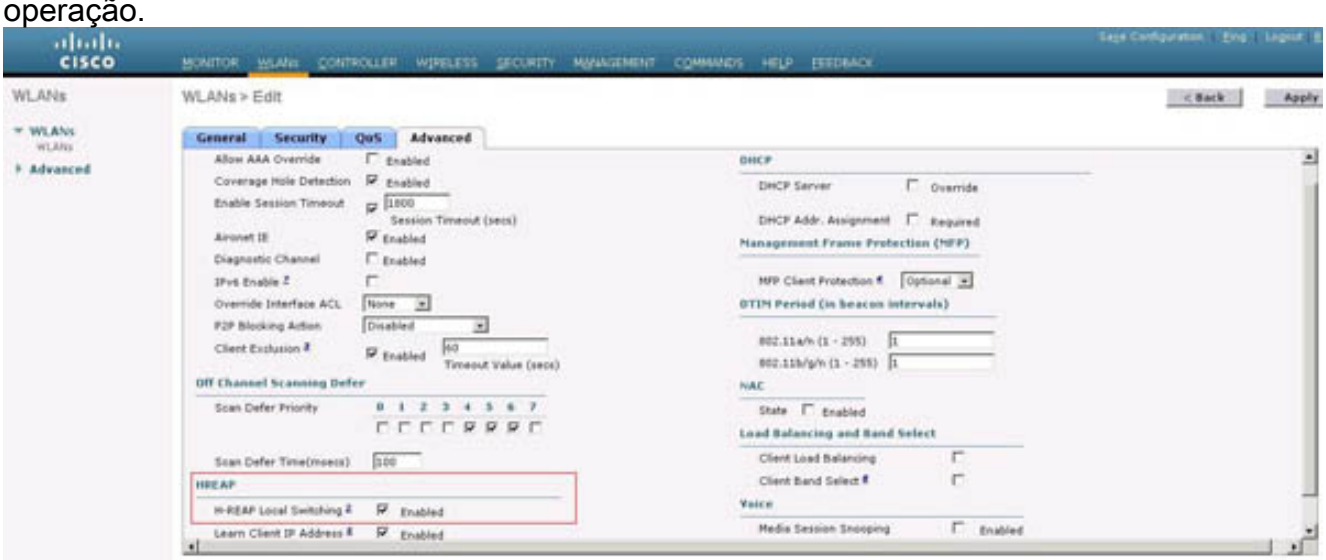
1. Vá à página principal do controlador, escolha **WLAN**, e clique **novo**.
2. Atribua ao WLAN um nome, que seja usado igualmente como o SSID, e o clique **aplica-se**.

3. No o WLAN > edita a página, clica a **ABA de segurança**. Sob a Segurança da camada 2,

selecione o tipo da Segurança.Para este exemplo, WPA2-PSK é desejado. Escolha **WPA+WPA2**.

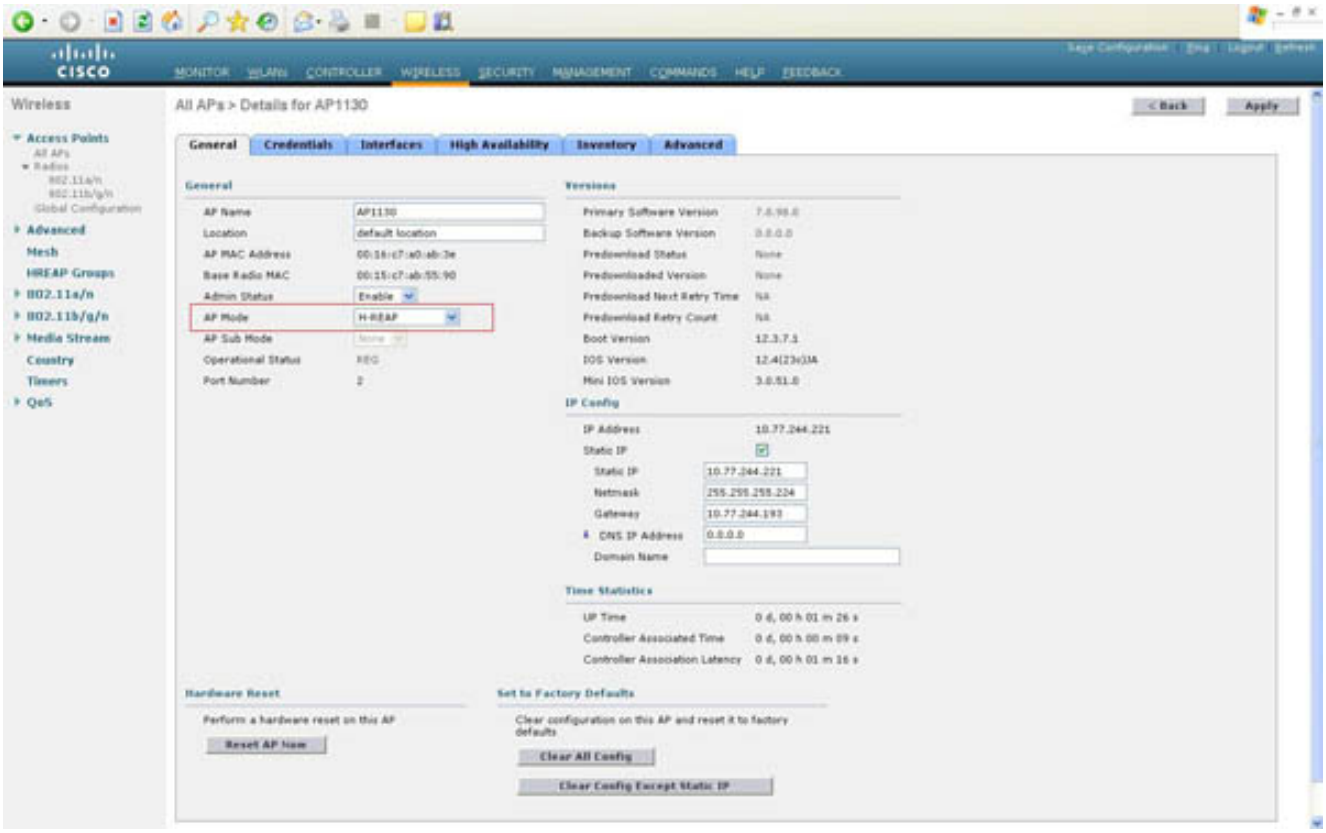


4. Verifique a **política WPA2** a fim especificar as operações WPA do WLAN.
5. Verifique o **AES** a fim ajustar o método de criptografia.
6. Sob a chave Mgmt do AUTH, escolha o **PSK do** menu suspenso.Segundo o formato chave desejado, a escolha aqui articula-se na acessibilidade e no suporte ao cliente, seleciona-se o **ascii** ou **encanta-se**. O ascii é tipicamente mais fácil porque os caráteres alfanuméricos são aceitados. Escolha o **ascii** e incorpore a chave pré-compartilhada desejada.
7. Clique na guia Advanced. A verificação **H COLHE o switching local** e assegura-se de que o WLAN esteja permitido para a operação.

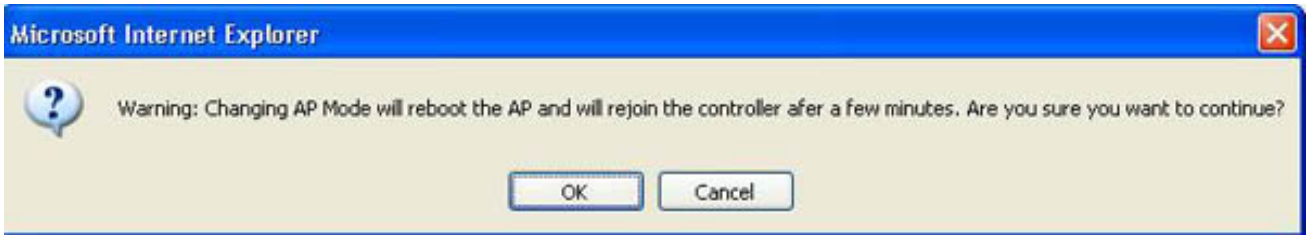


Sem esta etapa, o WLAN não permite que os dados estejam terminados localmente em H COLHE Access point ou não está oferecido de todo quando o Access point reage do modo independente.**Nota:** Os Access point não configurados para operar-se em H COLHEM o modo ignoram o H COLHEM o ajuste do switching local e todo o tráfego do cliente é escavado um túnel de volta ao controlador.Com o H COLHA O WLAN completo setup, o Access point pode então ser configurado para operar-se em H COLHEM o modo.

8. Depois que o Access point descobriu e se juntou ao controlador, vá à Web GUI do controlador sob o título wireless e clique o **detalhe** ao lado do Access point da escolha.
9. Pelo modo AP que dirige, escolha **H COLHEM do** menu suspenso a fim mudar o Access point de sua operação do modo local do padrão para funcionar em H COLHEM o modo.

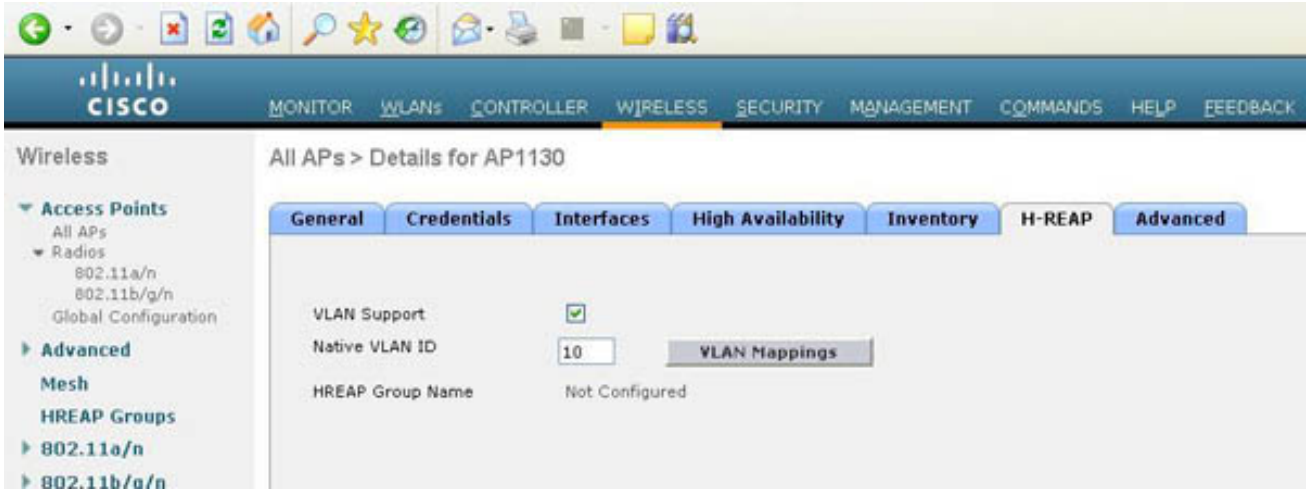


10. Clique em Apply. O Access point precisa de recarregar para que a configuração de modo tome o
efeito.

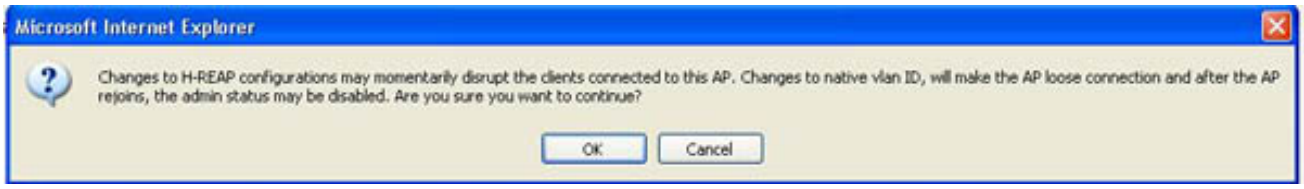


O Access point recarrega, redescobre o controlador, e junta-se ao controlador outra vez.

11. Retorne ao título **wireless do** controlador GUI e selecione o mesmo link do **detalhe do** Access point, como feito antes.Àrevelia, o H REAP não é configurado para operar sobre um enlace de tronco. Embora o switchport a que é conectado pode ser ajustado a um enlace de tronco, o Access point ainda comunica-se com o controlador sobre o VLAN nativo. Se o switchport é um enlace de tronco e se deseja mandar o H REAP se operar neste modo, o suporte de VLAN deve ser permitido.
12. Clique o **H COLHEM a** aba. Verifique o **suporte de VLAN**.
13. Baseado na configuração do switchport a que o H REAP é conectado, entre o número de ID do VLAN nativo do Access point ao lado do título com o mesmo nome (neste exemplo, VLAN10).

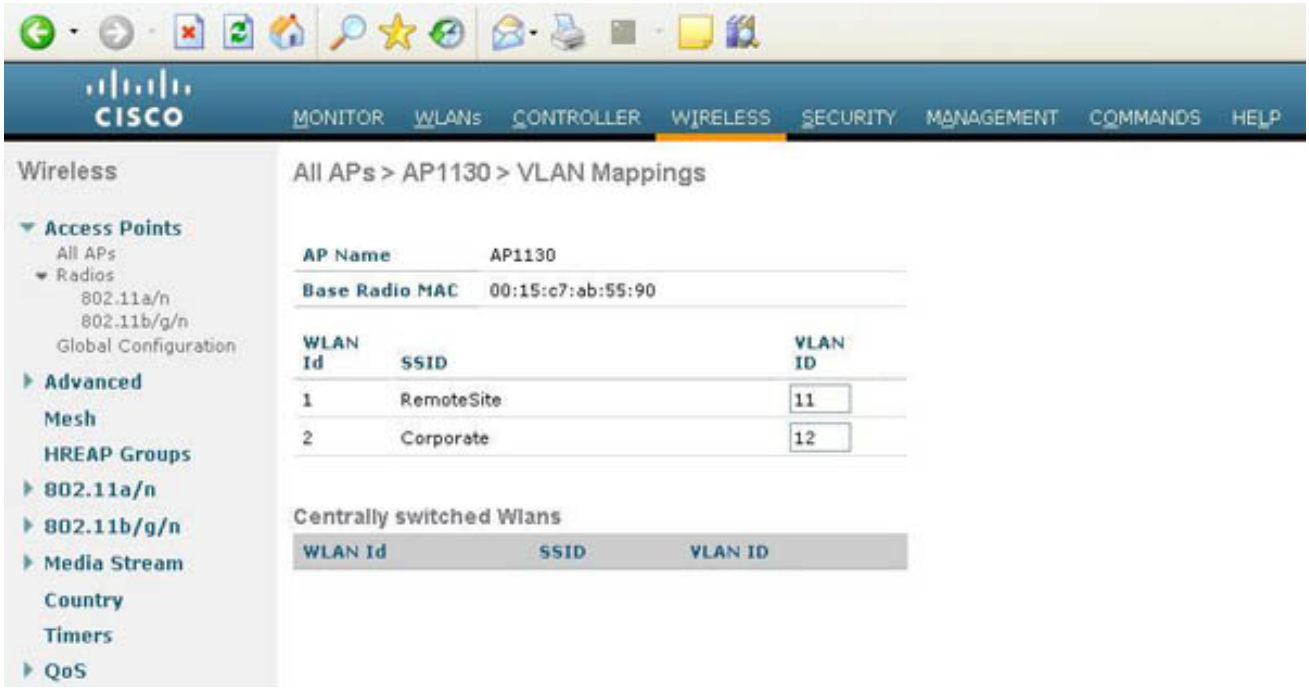


14. O clique **aplica-se** a fim decretar as mudanças.Porque o H COLHE restaurações a configuração de sua porta Ethernet baseada nos parâmetros de configuração dados, o Access point pode momentaneamente perder a Conectividade com o controlador. Uma janela pop-up adverte desta possibilidade. Clique em **OK**.



Nota: Porque o aviso emergente indica, há uma pequena possibilidade que o Access point tornará a reunir o controlador no estado desabilitado. Reselect que os **detalhes do** Access point ligam do título wireless do controlador. Selecione então **permitem** ao lado do status administrativo. Aplique o ajuste e continue com a configuração.

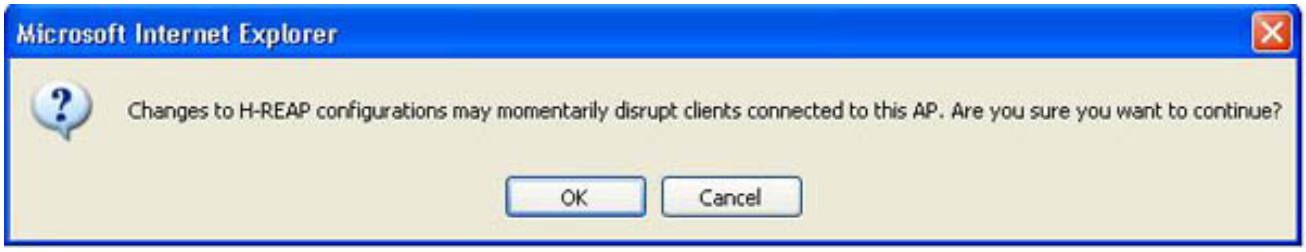
15. Entre na página do detalhe do Access point desejado, selecione o H COLHEM a etiqueta outra vez, e clicam o **mapeamento VLAN** a fim configurar o 802.1Q que etiqueta pelo WLAN localmente comutado.



16. Ajuste o VLAN pelo WLAN localmente comutado em que o tráfego do cliente deve ser terminado.**Nota:** Os WLAN não configurados para apoiar H COLHEM o switching local não permitem que a etiqueta do 802.1Q seja configurada aqui. A configuração de VLAN para

estes WLAN é ajustada nas configurações globais do controlador porque os dados do cliente são escavados um túnel de volta ao controlador para a terminação.**Nota:** Os WLAN localmente comutados enlatam toda a parte o mesmo ID de VLAN ou podem ter atribuições discretas. Não há nenhuma limitação aqui, desde que o vlan designada esta presente no switchport do H COLHE.

17. Clique em **Apply** para salvar as alterações.O serviço WLAN está interrompido momentaneamente quando o mapeamento VLAN/WLAN for mudado. **APROVAÇÃO do** clique para reconhecer
isto.



Os WLAN necessários são criados e configurado, os Access point ajustados para operar-se em H COLHEM o modo, o suporte de VLAN permitido, e os VLAN configurados pelo WLAN localmente comutado. Desde que os serviços DHCP estão disponíveis em cada VLAN, os clientes devem poder conectar a cada WLAN, recebem endereços em seus VLAN respectivos, e passam o tráfego. O H COLHE a configuração está agora completo.

Pesquisando defeitos H-REAP

Há alguns cenários comuns e as situações que elevaram e impedem H liso COLHEM a configuração e a conectividade de cliente. Esta seção fornece algumas tais situações seus remédios sugeridos.

H-REAP não se está juntando ao controlador

Isto pode ocorrer por vários motivos. Comece verificando o seguinte:

- **Cada H COLHE necessidades para ser corretamente IP endereçado.**Se o DHCP é usado através do console do Access point, verifique que o Access point obtém um endereço.
  ```
  AP_CLI#show dhcp lease
  ```

  Se o endereçamento estático é usado através do console do Access point, a verificação para certificar-se do endereçamento de IP correto é aplicada.
  ```
  AP_CLI#show capwap ip config
  ```

- **Assegure-se de que o Access point tenha a conectividade IP e possa sibilar a interface de gerenciamento do controlador.**Uma vez que o endereçamento de IP é verificado, a verificação para certificar-se do Access point pode comunicar-se com o controlador sibilando o endereço IP de gerenciamento do controlador. Use o **comando ping** através do console do Access point com esta sintaxe:
  ```
  AP_CLI#ping <WLC management IP address>
  ```

  Se isso não é bem sucedido, assegure-se de que a rede upstream esteja configurada corretamente e esse acesso WAN de volta à rede corporativa esteja disponível. Verifique que o controlador é operacional e não é atrás de nenhuns limites NAT/PAT. Assegure-se de que

as portas 5246 e 5247 UDP estejam abertas em todos os Firewall intermediários. Sibile do controlador ao Access point com a mesma sintaxe.

- **Verifique que há uma Conectividade CAPWAP entre o Access point e o controlador.**Uma vez a conectividade IP entre o H COLHE e o controlador é verificado, executa CAPWAP debuga no controlador para confirmar mensagens CAPWAP é comunicado através de WAN e para identificar problemas relacionados. No controlador, crie primeiramente um filtro MAC para limitar o espaço do resultado do debug. Use este comando a fim limitar a saída do comando subsequente a um único Access point.

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

  Ajuste uma vez para limitar o resultado do debug, gerenciem sobre a eliminação de erros CAPWAP.

  ```
  AP_CLI#debug capwap events enable
  ```

  Se nenhum CAPWAP debuga as mensagens estão consideradas, asseguram-se de que o H REAP tenha pelo menos um método por que um controlador pode ser descoberto. Se tais métodos são no lugar (como a opção de DHCP 43 ou DNS), verifique que estão configurados corretamente. Se nenhum outro método heurístico é no lugar, assegure-se de que o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador esteja incorporado no Access point através do console CLI.

  ```
  AP_CLI#capwap ap controller ip address <WLC management IP address>
  ```

- **Verifique operações CAPWAP no controlador e o H COLHE.**Se pelo menos um único método heurístico do controlador está disponível ao H COLHA, verifique que mensagens CAPWAP estão enviados do Access point ao controlador. Este comando é permitido já à revelia.

  ```
  AP_CLI#debug capwap client errors
  ```

  A informação adicional sobre que controladores o Access point comunica com pode ser considerada pelos endereços IP de Um ou Mais Servidores Cisco ICM NT do mensagem UDP que envia. Veja os endereços de rementente e destinatário de cada pacote que atravessa a pilha de IP do Access point.

  ```
  AP_CLI#debug ip udp
  ```

  Se parece do console do Access point que se comunica com um controlador, é possível que se juntou a um outro controlador no conjunto. A fim verificar se o H REAP é conectado a um controlador, use este comando.

  ```
  AP_CLI#show capwap reap status
  ```

- **Verifique que o Access point se juntou ao controlador correto.**Se outros endereços IP de Um ou Mais Servidores Cisco ICM NT do controlador são entregados ao Access point durante a fase da descoberta, o H REAP pode ter-se juntado a um outro controlador. Verifique que o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador feito disponível pelo mecanismo de descoberta está correto. Identifique o controlador a que o Access point se juntou.

  ```
  AP_CLI#show capwap reap status
  ```

  Log nessa Web GUI do controlador. Assegure-se de que todos os endereços IP e MAC dos controladores estejam incorporados na lista da mobilidade do controlador e isso todos compartilhem do mesmo nome do grupo da mobilidade. Então, ajuste o Access point

preliminares, secundários, e controladores terciários para ditar que controlador o Access point se junta. Isto é feito através do link dos detalhes do Access point. Se o problema descansa com o H REAP que se junta a um outro controlador, este pode extremamente ser facilitado usando as potencialidades de gerenciamento sistema-largas do Access point WCS.
- **Pesquise defeitos edições do certificado se o Access point está tentando se juntar ao controlador, mas falhe.**Se as mensagens CAPWAP estão consideradas no controlador, mas o Access point não se junta, este provável é uma edição do certificado.

Os comandos console de H-REAP não são operacionais e retornam um erro

Todos os comandos configuration (ajuste ou esclarecimento da configuração) executaram com o H COLHEM o retorno CLI o `ERRO!!! O comando é` mensagem `desabilitada`. Isto pode acontecer para uma de duas razões:

- H COLHE os Access point que reagem do modo conectado não permitirão o ajuste ou o esclarecimento de todas as configurações através do console. Quando o Access point está neste estado, as configurações devem ser feitas através da relação do controlador. Se o acesso aos comandos configuration no Access point é exigido, assegure-se de que o Access point reaja do modo independente antes de tentar inscrever todos os comandos configuration.
- Uma vez que o Access point conectou a um controlador em qualquer momento (mesmo se o H REAP se moveu de volta ao modo independente), o console do Access point não permitirá comandos configuration até que uma senha nova esteja ajustada. Cada a senha H REAP precisa de ser mudada. Isto pode somente ser ajustado com o CLI do controlador a que o Access point é conectado. Esta sintaxe de comando pode ser usada no controlador para ajustar a senha de console ou a senha de um ponto de acesso individual aos Access point de todo o controlador:
  `(WLC_CLI)>`**`config ap username <user-id> password <passwd> {all | <AP name>}`**

  Nota: Para um Access point que não tenha suas senhas de console ajustadas, esteja ciente que esta configuração está enviada somente ao Access point no ponto que o comando é incorporado no controlador. Todos os Access point que se juntarem subseqüentemente a este exigirão o comando sejam entrados outra vez.Mesmo uma vez que o Access point ambos esteve dado uma senha não-padrão e o Access point reage do modo independente, o Access point ainda assim não permitirá o acesso a estes comandos. A fim fazer mudanças à configuração H o REAP, a remoção de endereçamento PRE-existente do IP Estático e as configurações de endereço IP do controlador são exigidas. Esta configuração está chamada a configuração privada CAPWAP e deverá ser removida antes que todos os comandos CLI novos do Access point possam ser entrados. A fim fazer isto, incorpore este comando:
  `AP_CLI#`**`clear capwap private-config`**

  Nota: Alternativamente, o AP pode ser retornado aos padrões de fábrica quando for juntado a um controlador. Clique o botão **claro da configuração na** página dos detalhes do AP sob o título wireless no WLC GUI. A configuração do AP é limpada e é recarregada.**Nota:** Todos os **comandos show and debug** continuarão a trabalhar mesmo sem uma senha não-padrão que está sendo ajustada e com o AP no modo conectado.Somente neste momento podem todas as configurações CAPWAP ser feitas.

Os clientes não podem conectar ao H-REAP

Conclua estes passos:

1. Verifique que o Access point se juntou corretamente ao controlador, o controlador tem pelo menos um (e permitido) WLAN corretamente configurado, e se assegura de que o H REAP esteja no estado permitido.
2. Na extremidade do cliente, verifique que o SSID do WLAN está disponível (no controlador, configurar o WLAN para transmitir seu SSID pode ajudar este processo de Troubleshooting). Espelhe a configuração de segurança do WLAN no cliente. As configurações de segurança do lado do cliente são onde a grande maioria dos problemas de conectividade reside.
3. Assegure-se de que os clientes em WLAN localmente comutados sejam corretamente IP endereçado. Se o DHCP é usado, certifique-se que um servidor DHCP ascendente é configurado corretamente e de fornecimento endereços aos clientes. Se o endereçamento estático é usado, assegure-se de que os clientes estejam configurados corretamente para a sub-rede correta.
4. A fim pesquisar defeitos mais edições da conectividade de cliente na porta de Console H o REAP, incorpore este comando.
   AP_CLI#**show capwap reap association**

5. A fim pesquisar defeitos mais edições da conectividade de cliente no controlador e limitar a saída de uma eliminação de erros mais adicional, use este comando.
   AP_CLI#**debug mac addr <client's MAC address>**

6. A fim debugar problemas de conectividade do 802.11 de um cliente, use este comando.
   AP_CLI#**debug dot11 state enable**

7. Debugar o processo de autenticação e as falhas do 802.1X de um cliente com este comando.
   AP_CLI#**debug dot1x events enable**

8. As mensagens backend controller/RADIUS podem ser debugadas usando este comando.
   AP_CLI#**debug aaa events enable**

9. Alternativamente, para permitir um terno completo de comandos debug do cliente, use este comando.
   AP_CLI#**debug client <client's MAC address>**

H-REAP QA

Q. Se eu configuro regaços em uma posição remota enquanto H colhe, posso eu dar 2 aqueles regaços um controlador principal e secundário?

Exemplo: Há um controlador principal no local A e um controlador secundário no local B.

Se o controlador no local A falha, o REGAÇO faz o Failover ao controlador no local B. Se ambos os controladores são não disponíveis fazem a queda do REGAÇO em H COLHEM o modo local?

A. Yes. Primeiramente o REGAÇO falha sobre ao seu secundário. Todos os WLAN que são comutados localmente não têm nenhuma mudança, e todo o que é comutada centralmente apenas mandam o tráfego ir ao controlador novo. E, se o secundário falha, todos os WLAN que

são marcados para o switching local (e abra/autenticação da chave pré-compartilhada/você estão fazendo o autenticador AP) permanecem acima.

Q. Como os Access point configurados no negócio do **modo local** com os WLAN configurados com H COLHEM o switching local?

A. Os pontos de acesso de modo locais tratam estes WLAN como WLAN normais. A autenticação e o tráfego de dados são escavados um túnel de volta ao WLC. Durante uma falha do link MACILENTO este WLAN está completamente para baixo e nenhum cliente é ativo neste WLAN até que a conexão ao WLC esteja restaurada.

Q. Posso eu fazer a autenticação da Web com switching local?

Sim, você pode ter um SSID com a autenticação da Web permitida e deixar cair o tráfego localmente após a autenticação da Web. A autenticação da Web com switching local trabalha muito bem.

Q. Posso eu usar meu Convidado-portal no controlador para um SSID, que seja segurado localmente pelo H COLHA? Se sim, que acontece se eu perco a Conectividade ao controlador? Os clientes atual deixam cair imediatamente?

Yes. Desde que este WLAN é comutado localmente, o WLAN está disponível mas nenhum cliente novo pode autenticar porque o página da web não está disponível. Contudo, os clientes existentes não são deixados cair fora.

Informações Relacionadas

- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Atualização do software do Wireless LAN Controller (WLC)
- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Suporte por tecnologia WLAN
- H COLHE o modo de exemplo de configuração da operação
- Troubleshooting básico remoto híbrido do Access point da borda (H COLHE)
- Exemplos e TechNotes da configuração de controle do Wireless LAN
- Erro do controlador do Wireless LAN (WLC) e mensagens de sistema FAQ
- Erro wireless e mensagens de sistema do sistema de controle (WCS)
- Suporte Técnico e Documentação - Cisco Systems