Modo H-REAP de exemplo de configuração da operação

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Informações de Apoio
H-REAP sobre COLHEM
Configurar
Diagrama de Rede
Configuração
Aprontando o AP com um controlador e configurar H-REAP
Teoria da operação H-REAP
Estados do interruptor H-REAP
Autenticação central, interruptor central
Verifique a autenticação central, interruptor central
Autenticação para baixo, comutando para baixo
Autenticação central, switching local
Verifique a autenticação central, switching local
Autenticação para baixo, switching local
Autenticação local, switching local
Verifique a autenticação local, switching local
Troubleshooting
Informações Relacionadas

Introdução

Este documento introduz o conceito de Ponto de Acesso Remoto Híbrido da Borda (H-REAP) e explica seus diferentes modos de operação com uma configuração de exemplo.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento dos controladores do Wireless LAN (WLC) e como configurar os parâmetros

básicos WLC
- O conhecimento de COLHE

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa a versão de firmware 7.0.116.0
- Access point de pouco peso de Cisco 1131AG (REGAÇO)
- Cisco 2800 Series Router que executam a versão 12.4(11)T.
- Adaptador cliente do Cisco Aironet 802.11a/b/g que executa a versão de firmware 4.0
- Versão de utilitário de desktop 4.0 do Cisco Aironet
- Cisco Secure ACS que executa a versão 4.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

H-REAP é uma solução Wireless para disposições do escritório filial e do escritório remoto. H-REAP permite clientes de configurar e controlar os Access point (AP) em um ramo ou em um escritório remoto do escritório corporativo através de um link MACILENTO sem distribuir um controlador em cada escritório.

H-Colher pode comutar o tráfego de dados do cliente localmente e executar a authenticação do cliente localmente quando a conexão ao controlador é perdida. Quando conectados ao controlador, os H-REAPs também podem enviar o tráfego por túnel de volta ao controlador. No modo conectado, o híbrido COLHE O AP pode igualmente executar a autenticação local.

H-REAP é apoiado somente sobre:

- 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040, e AP3550 AP
- Cisco 5500, 4400, 2100, 2500, e do 7500 Series do cabo flexível controladores
- Interruptor integrado 3750G do controlador do catalizador
- Módulo de Serviços sem fio do Catalyst 6500 Series (WiSM)
- Módulo do controlador do Wireless LAN (WLCM) para o Roteadores dos Serviços integrados (ISR)

O tráfego do cliente H-Colher pode ser comutado localmente no AP ou ser escavado um túnel de volta a um controlador. Isto depende da configuração por-WLAN. Também, o tráfego localmente comutado do cliente no H-REAP pode ser 802.1Q etiquetado para prever a separação do prender-lado. Durante a interrupção de WAN, o serviço em tudo comutado localmente, WLAN localmente autenticados persiste.

Nota: Se os AP reagem do modo H-REAP e são comutados localmente no local remoto, a atribuição dinâmica de usuários a um VLAN específico baseado na configuração de servidor RADIUS não está apoiada. Contudo, você deve poder atribuir usuários aos VLAN específicos baseados no VLAN estático ao traço do Service Set Identifier (SSID) feito localmente no AP. Consequentemente, um usuário que pertença a um SSID particular pode ser atribuído a um VLAN específico a que o SSID é traçado localmente no AP.

Nota: Se a Voz sobre o WLAN é importante, a seguir os AP devem ser executados no modo local de modo que obtenham o CCKM e o apoio do controle de admissão de conexão (CAC), que não são apoiados no modo H-REAP.

H-REAP sobre COLHEM

Refira a Remoto-borda AP (COLHA) com AP de pouco peso e o exemplo de configuração dos controladores do Wireless LAN (WLC) para que mais informação ajude a compreender COLHEM.

H-REAP foi introduzido em consequência destes defeitos REAP:

- REAP não tem a separação do prender-lado. Isto é devido faltar do apoio do 802.1Q. Os dados dos WLAN aterram na mesma sub-rede prendida.
- Durante uma falha WAN, uma COLHEITA AP cessa o serviço oferecido em todos os WLAN, a não ser que primeiro especifique no controlador.

Isto é como H-REAP supera estes dois defeitos:

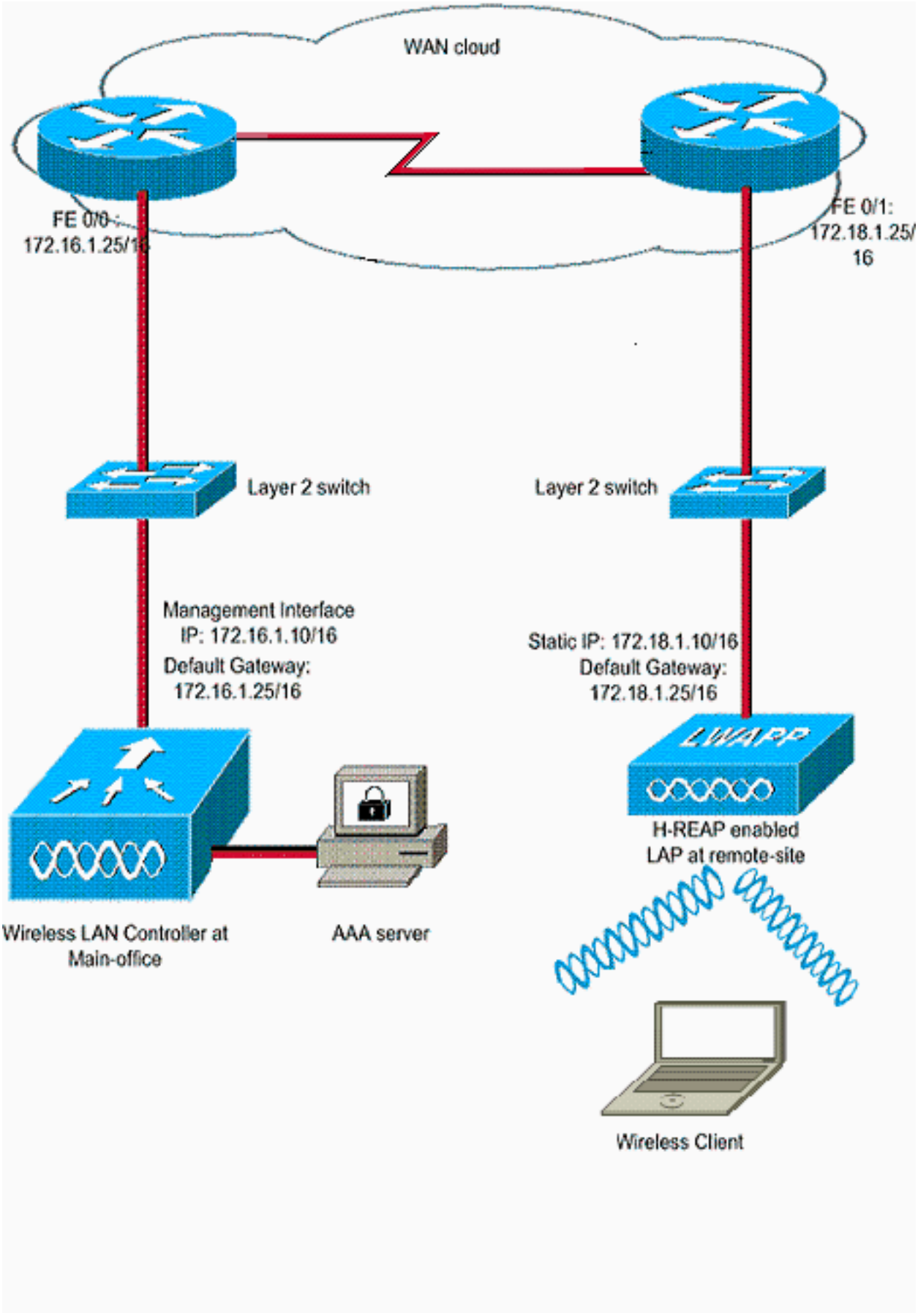
- Fornece o apoio do dot1q e o VLAN ao mapeamento SSID. Este VLAN ao mapeamento SSID precisa de ser feito em H-REAP. Quando você executar este, assegure-se de que os VLAN configurados estejam permitidos corretamente através das portas no Switches e no Roteadores intermediários.
- Proporciona o serviço contínuo a todos os WLAN configurados para o switching local.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração

Este exemplo supõe que o controlador está configurado já com configurações básicas. O controlador usa estas configurações:

- Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento — 172.16.1.10/16
- Endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do gerenciador AP — 172.16.1.11/16
- Endereço IP de roteador do gateway padrão — 172.16.1.25/16
- Endereço IP de Gateway virtual — 1.1.1.1

Nota: Este documento não mostra as configurações de WAN e a configuração do roteador e o Switches disponíveis entre o H-REAP e o controlador. Isto supõe que você está ciente do Encapsulamento de WAN e dos protocolos de roteamento que são usados. Também, este documento supõe que você compreende como os configurar a fim manter a Conectividade entre o H-REAP e o controlador através do link MACILENTO. Neste exemplo, o encapsulamento de HDLC é usado no link MACILENTO.

Aprontando o AP com um controlador e configurar H-REAP

Se você quer o AP descobrir um controlador de uma rede remota onde os mecanismos de descoberta CAPWAP não estejam disponíveis, você pode usar a escorva. Este método permite-o de especificar o controlador a que o AP deve conectar.

A fim aprontar um AP H-COLHER-capaz, conecte o AP à rede ligada com fio no escritório principal. Durante sua bota acima, o AP H-COLHER-capaz procura primeiramente um endereço IP de Um ou Mais Servidores Cisco ICM NT para se. Uma vez que adquire um endereço IP de Um ou Mais Servidores Cisco ICM NT através de um servidor DHCP, carreg acima e procura um controlador para executar o processo de registro.

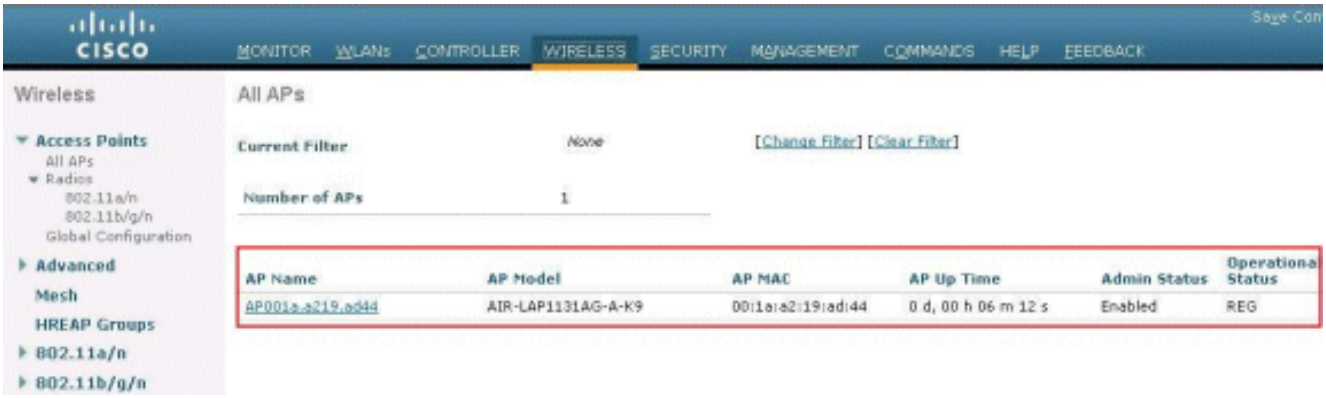
Um H-REAP AP pode aprender o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador em algumas das maneiras explicadas no registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (WLC).

Nota: Você pode igualmente configurar o REGAÇO para descobrir o controlador através dos comandos CLI no AP. Refira a descoberta do controlador H-REAP usando comandos CLI para mais informação.

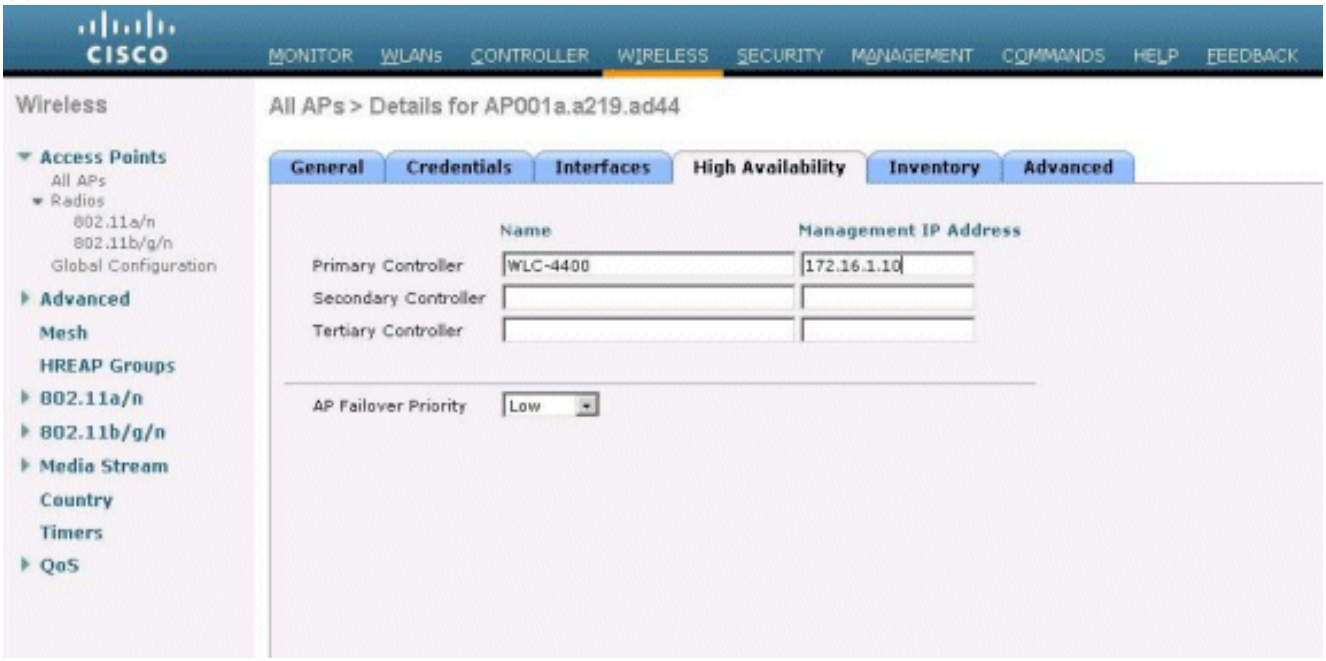
O exemplo neste documento usa o procedimento da opção de DHCP 43 para que o H-REAP aprenda o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador. Então junta-se ao controlador, transfere-se a imagem do software mais recente e a configuração do controlador, e inicializa-se o link de rádio. Salvar a configuração transferida na memória permanente para o uso no modo independente.

O REGAÇO é registrado uma vez com o controlador, termina estas etapas:

1. No controlador GUI, escolha **pontos de Wireless>Access**.Isto indica o REGAÇO registrado com este controlador.
2. Clique sobre o AP que você quer configurar.

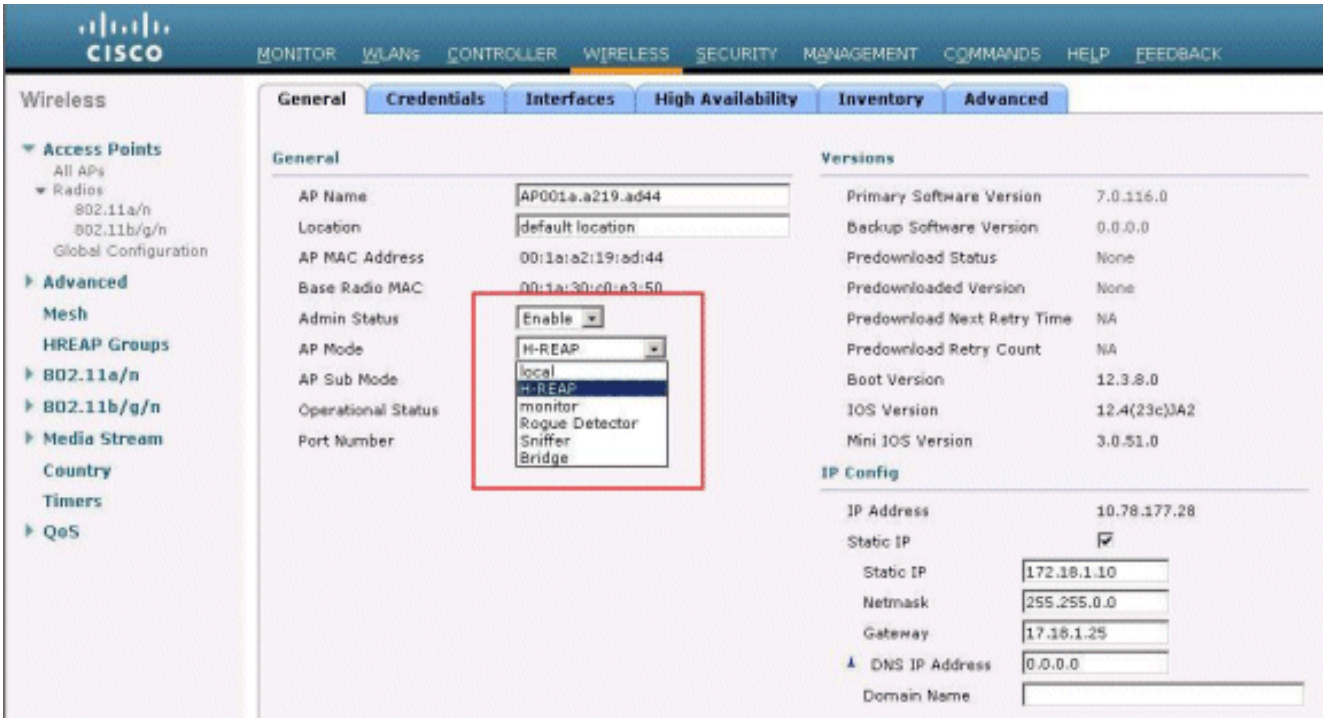


3. No indicador de APs>Details, clique sobre a Alta disponibilidade da aba, e defina os nomes do controlador que os AP se usarão para registrar, a seguir clicam **aplicam-se**.



Você pode definir até três nomes do controlador (preliminar, secundário, e terciário). Os AP procuram pelo controlador na mesma ordem que você fornece neste indicador. Porque este exemplo usa somente um controlador, o exemplo define o controlador como o controlador principal.

4. Configurar o REGAÇO para H-REAP.A fim configurar o REGAÇO para operar-se no modo H-REAP, no indicador de APs>Details, sob o tab geral, escolhe o **modo AP** enquanto H-REAP da correspondência deixam cair para baixo o menu.Isto configura o REGAÇO para operar-se no modo H-
REAP.



Nota: Neste exemplo, você pode ver que o endereço IP de Um ou Mais Servidores Cisco ICM NT do AP está mudado ao modo estático e o endereço IP estático 172.18.1.10 esteve atribuído. Esta atribuição ocorre porque esta é a sub-rede a ser usada no escritório remoto. Consequentemente, você usa o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP, mas somente durante a primeira vez através da fase do registro. Depois que o AP é registrado ao controlador, você muda o endereço a um endereço IP estático.

Agora que seu REGAÇO é aprontado com o controlador e configurado para o modo H-REAP, a próxima etapa é configurar H-REAP no lado do controlador e discutir os estados do interruptor H-REAP.

Teoria da operação H-REAP

O REGAÇO H-COLHER-capaz opera-se nestes dois modos diferentes:

- Modo **conectado**:Um H-REAP seriam no modo conectado quando seu link do plano do controle CAPWAP ao WLC é ascendente e operacional. Isto significa que o link MACILENTO entre o REGAÇO e o WLC não está para baixo.
- **Modo independente**:Um H-REAP seriam no modo independente quando seu link MACILENTO ao WLC está para baixo. Por exemplo, quando este H-REAP já não tiver a Conectividade ao WLC conectado através do link MACILENTO.

O mecanismo da autenticação usado para autenticar um cliente pode ser definido como a **central** ou o **Local**.

- **Autenticação central** — Refere o tipo do autenticação que envolve o processo do WLC do local remoto.
- **Autenticação local** — Refere os tipos do autenticação que não envolvem processar do WLC para a autenticação.

Nota: Toda a autenticação do 802.11 e processamento da associação ocorrem no H-REAP, nenhuma matéria em que o modo o REGAÇO está. Quando no modo conectado, nos proxys H-REAP então estas associações e nas autenticações ao WLC. No modo independente, o REGAÇO não pode informar o WLC de tais eventos.

Quando um cliente conecta a um H-REAP AP, o AP encaminha todos os mensagens de autenticação ao controlador. Após a autenticação bem sucedida, seus pacotes de dados são comutados então localmente ou escavados um túnel de volta ao controlador. Isto está do acordo à configuração do WLAN a que é conectada.

Com H-REAP, os WLAN configurados em um controlador podem ser operados em dois modos diferentes:

- **Interruptor central:**Um WLAN em H-REAP está dito operar-se no modo de switching central se o tráfego de dados desse WLAN é configurado para ser escavado um túnel ao WLC.
- **Switching local:**Um WLAN em H-REAP é dito operar-se no modo do switching local se o tráfego de dados desse WLAN termina localmente na relação prendida do REGAÇO própria, sem obter escavado um túnel ao WLC.**Nota:** Somente os WLAN 1 a 8 podem ser configurados para o switching local H-REAP porque somente estes WLAN podem ser aplicados aos 1130, o 1240 e 1250 Series AP que apoia a funcionalidade H-REAP.

Estados do interruptor H-REAP

Combinado com a autenticação e os modos de switching mencionados na seção anterior, um H-REAP pode operar-se em qualquens um estados:

- Autenticação central, interruptor central
- Autenticação para baixo, comutando para baixo
- Autenticação central, switching local
- Autenticação para baixo, switching local
- Autenticação local, switching local

Autenticação central, interruptor central

Neste estado, para o WLAN dado, o AP para a frente todos os pedidos da authenticação do cliente ao controlador e escava um túnel todos os dados do cliente ao WLC. Este estado é válido somente quando o H-REAP reage do modo conectado. Todo o WLAN que for configurado para se operar neste modo é perdido durante a interrupção de WAN, não importa o que o método de autenticação é.

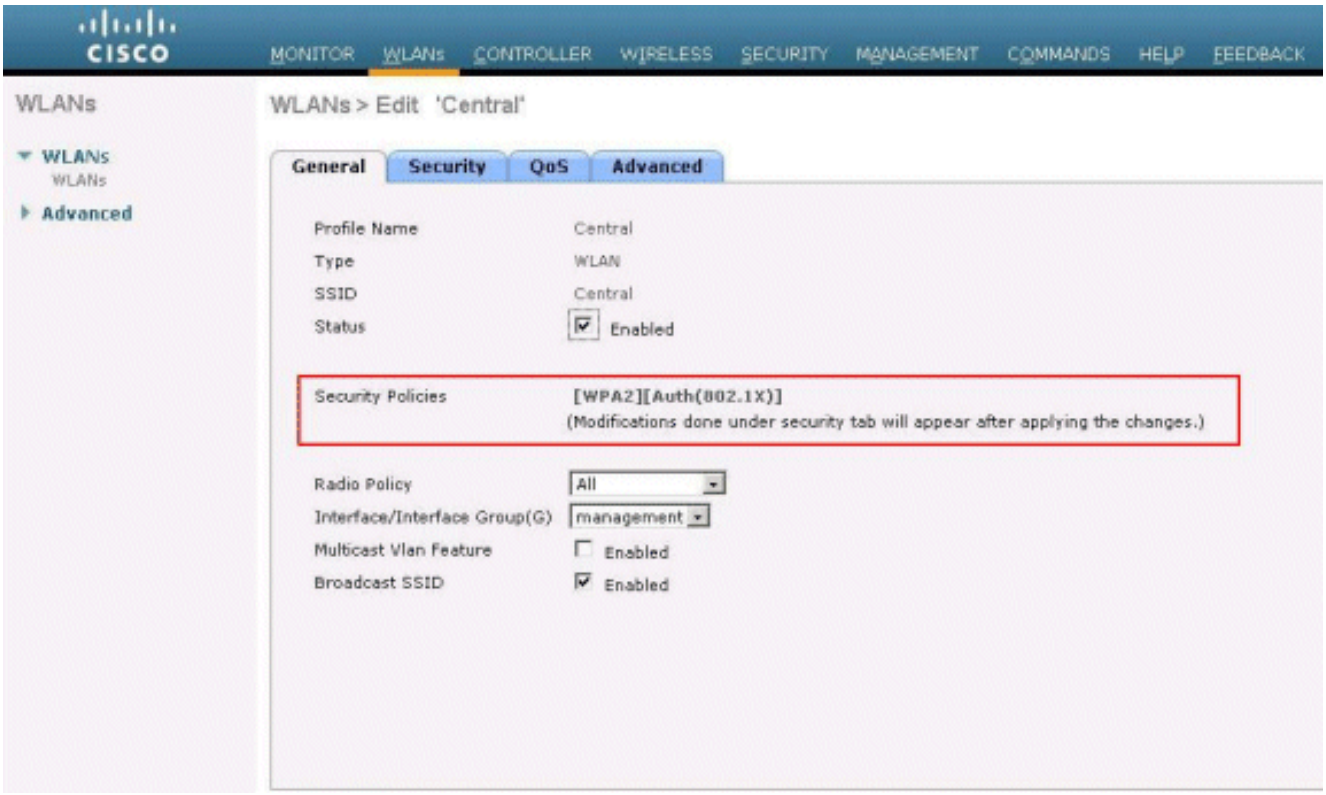
Este exemplo usa estes ajustes de configuração:

- Nome WLAN/SSID: **Central**
- Segurança da camada 2: **WPA2**
- Switching local H-REAP: **Desabilitado**

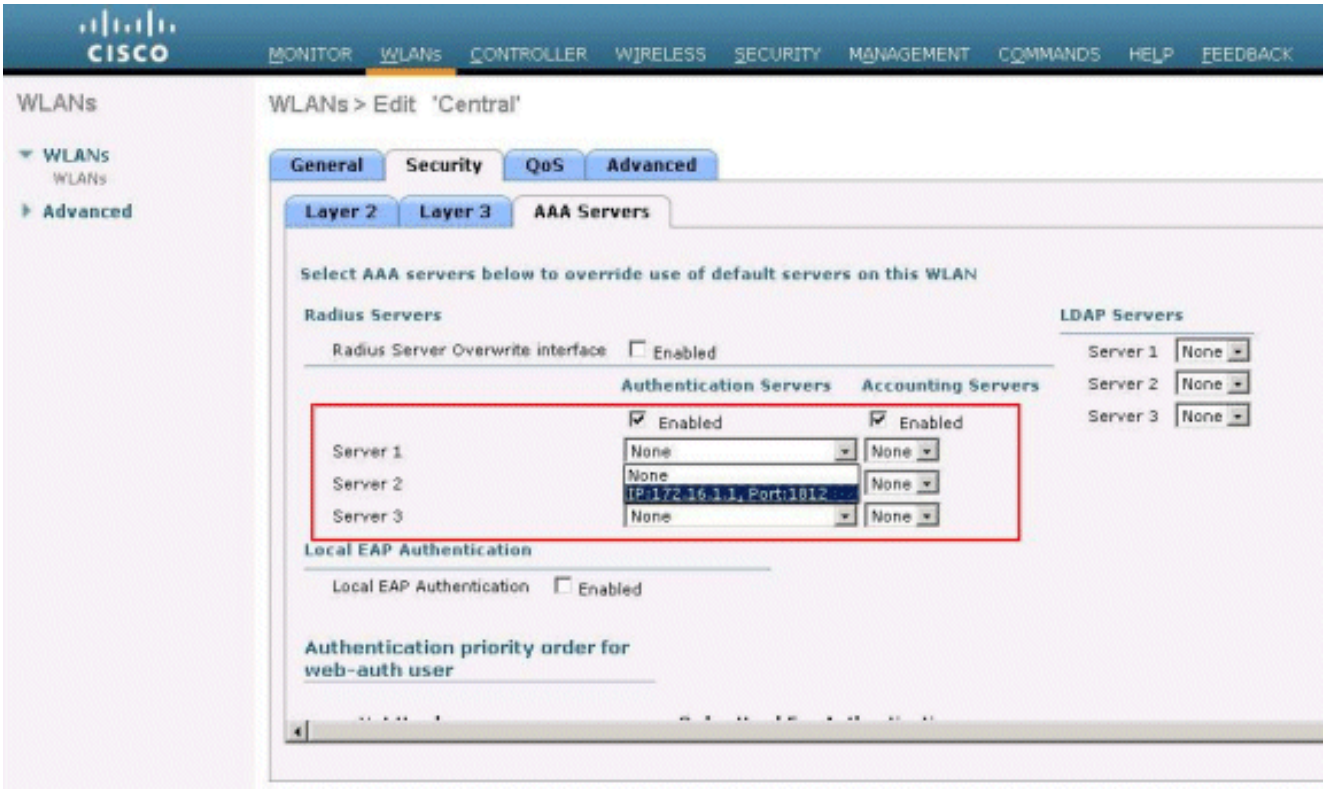
Termine estas etapas a fim configurar o WLC para a autenticação central, interruptor central usando o GUI:

1. Clique **WLAN** a fim criar um **Central** nomeado WLAN novo, a seguir clique-os **aplicam-se**.

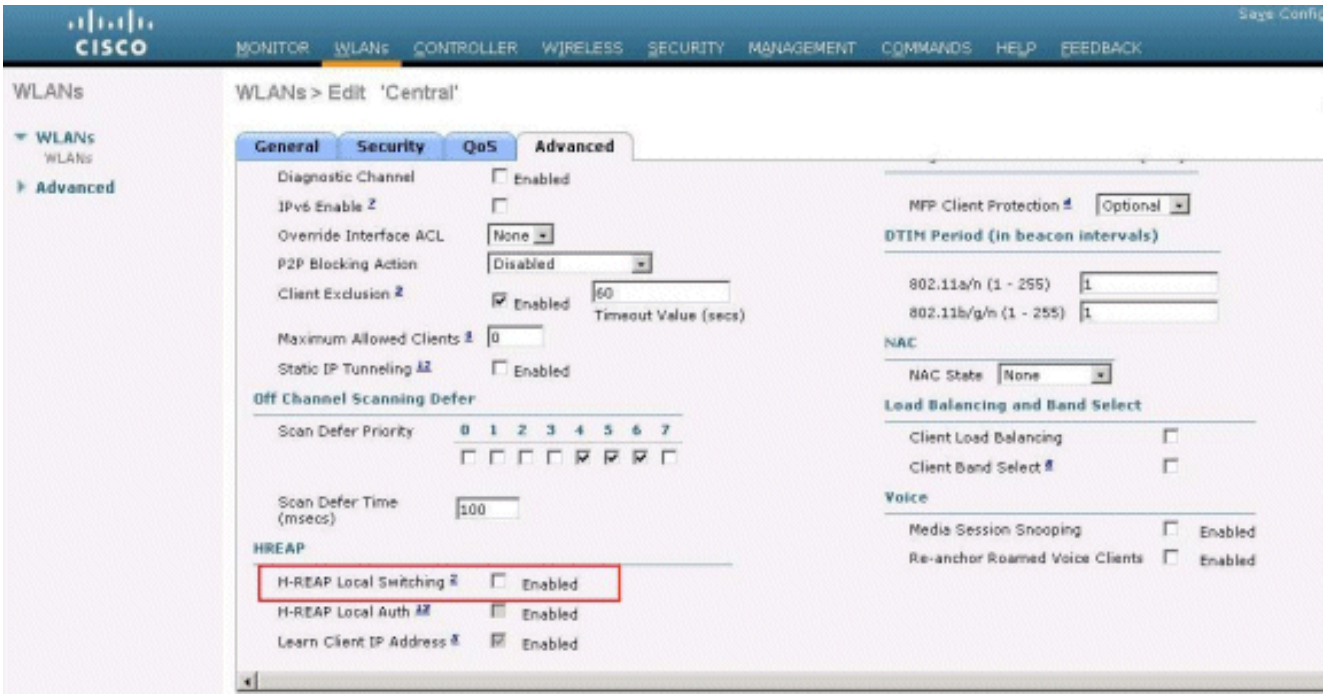
2. Porque este WLAN usa a autenticação central, nós usamos a autenticação WPA2 no campo de Segurança da camada 2. O WPA2 é a Segurança da camada 2 do padrão para um WLAN.



3. Escolha a aba dos servidores AAA, e escolha então o server apropriado configurado para a autenticação.



4. Porque este WLAN usa o interruptor central, você precisa de assegurar-se de que a caixa de verificação do switching local H-REAP esteja desabilitada (isto é a caixa de verificação do switching local não é selecionada). Então, o clique aplica-se.

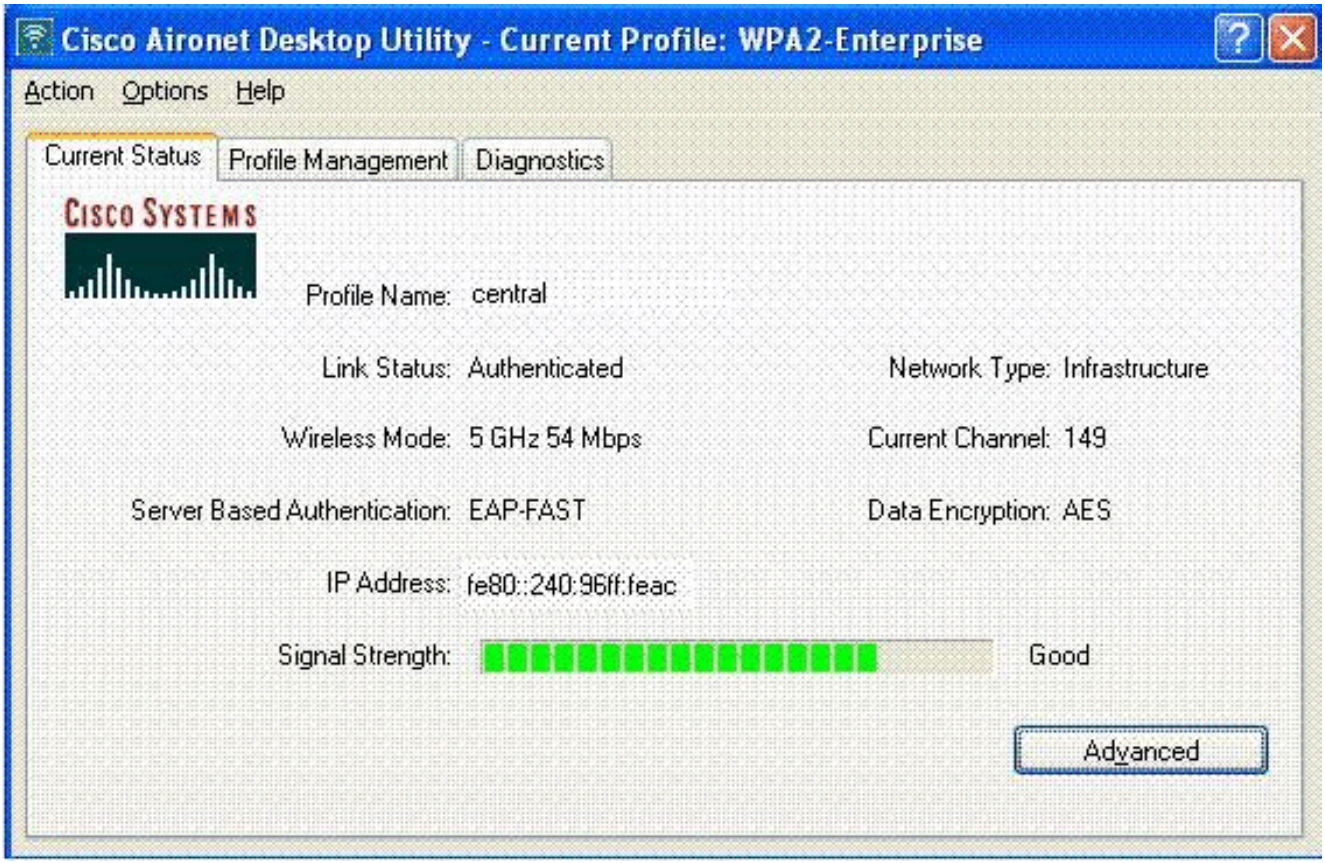


Verifique a autenticação central, interruptor central

Conclua estes passos:

1. Configurar o cliente Wireless com o mesmos SSID e configurações de segurança.Neste exemplo, o SSID é *central* e o método de segurança é *WPA2*.
2. Incorpore o nome de usuário e senha como configurado no server>User do RAIO Setup a fim ativar o SSID central no cliente.Este exemplo usa o *usuário1* como o nome de usuário e

senha. O cliente centralmente é autenticado pelo servidor Radius e associado com o H-REAP AP. O H-REAP está agora na **autenticação central, interruptor central**.



Autenticação para baixo, comutando para baixo

Com a mesma configuração explicada na autenticação central, a seção de interruptor central, desabilita o link MACILENTO que conecta o controlador. Agora, as esperas do controlador para uma pulsação do coração respondem do AP. Uma resposta da pulsação do coração é similar aos

mensagens de keepalive. O controlador tenta cinco heartbeats consecutiva, cada cada segundo.

Porque não é recebido com uma resposta da pulsação do coração do H-REAP, o WLC cancela a matrícula o REGAÇO.

Emita o **comando enable dos eventos do capwap debugar do** CLI do WLC a fim verificar o processo da cancelamento da matrícula. Esta é as saídas de exemplo deste **comando debug**:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP
00:15:c7:ab:55:90 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu
Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister
capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu
Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister
capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 0! Thu Jan 18 03:19:32 2007:
00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 0 Thu Jan 18 03:19:32
2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 1! Thu Jan 18
03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 1
```

O H-REAP entra no modo independente.

Porque este WLAN previamente foi autenticado centralmente e comutado centralmente, controle e o tráfego de dados foi escavado um túnel de volta ao controlador. Consequentemente, sem o controlador, o cliente é incapaz de manter a associação com o H-REAP e é desligado. Este estado de H-REAP com a associação de cliente e a autenticação que estão para baixo é referido como a autenticação para baixo, comutando para baixo.

Autenticação central, switching local

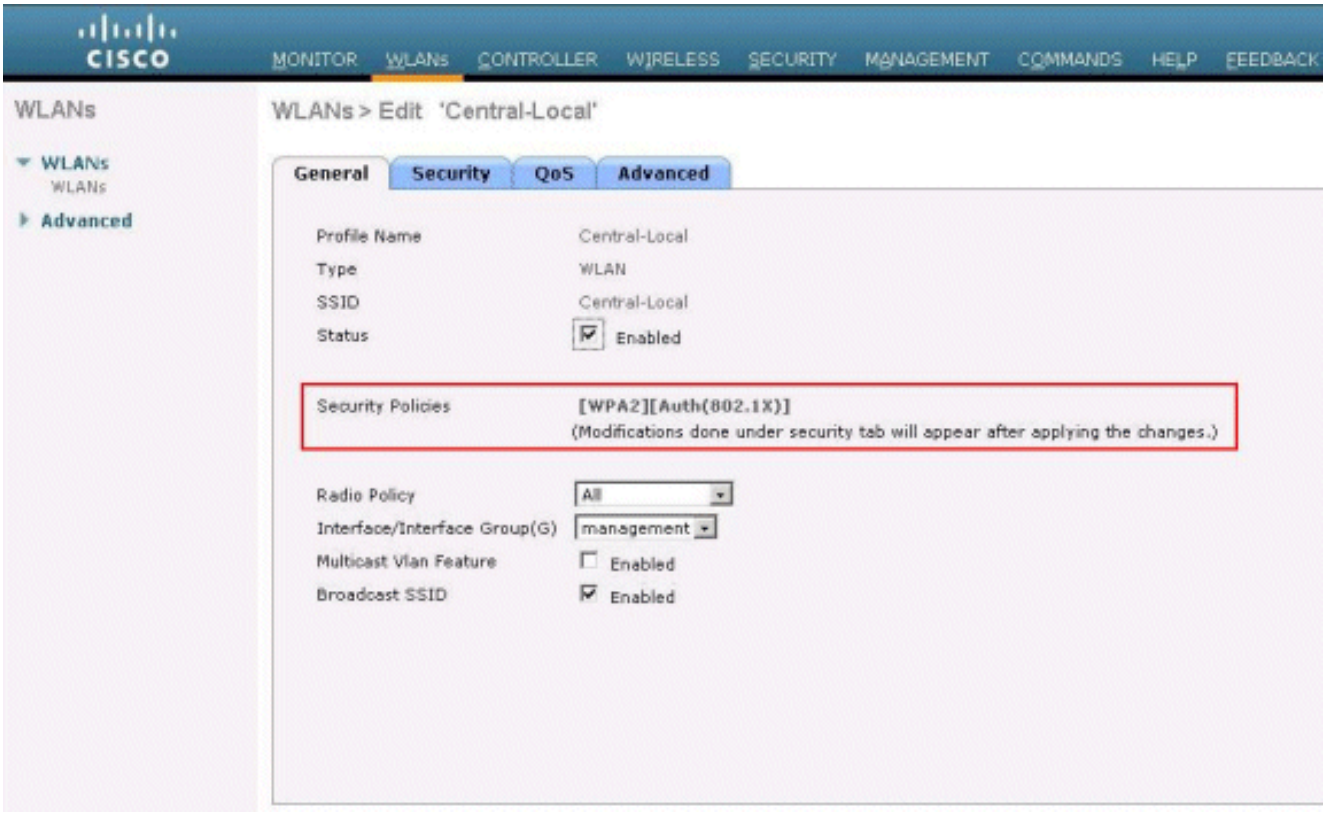
Neste estado, para o WLAN dado, o WLC segura toda a authenticação do cliente, e os pacotes de dados do Switches do REGAÇO H-REAP localmente. Depois que o cliente autentica com sucesso, o controlador envia comandos de controle do capwap ao H-REAP e instrui o REGAÇO para comutar que os pacotes de dados do cliente dado localmente. Esta mensagem é enviada pelo cliente em cima da autenticação bem sucedida. Este estado é aplicável somente no modo conectado.

Este exemplo usa estes ajustes de configuração:

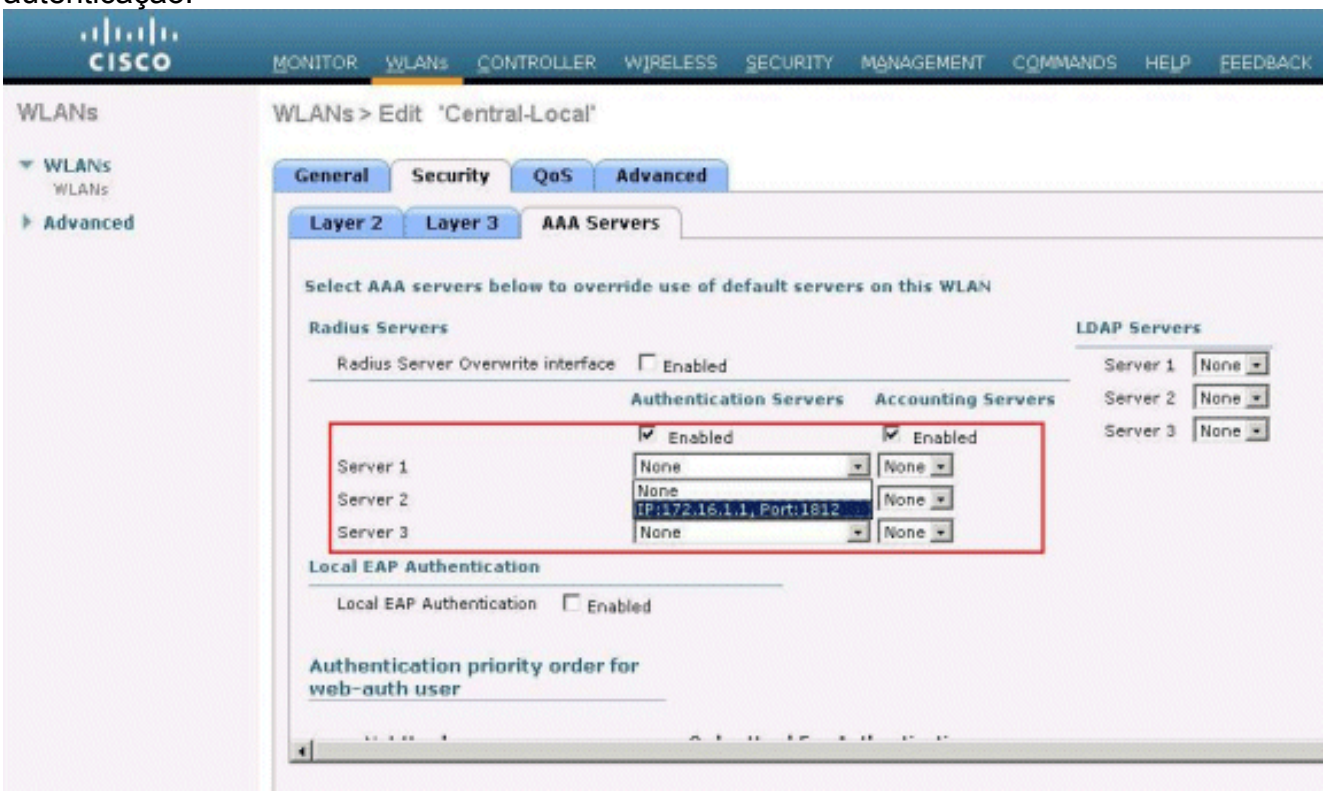
- Nome WLAN/SSID: **Central-local**
- Segurança da camada 2: **WPA2**.
- Switching local H-REAP: **Habilitado**

Do controlador GUI, termine estas etapas:

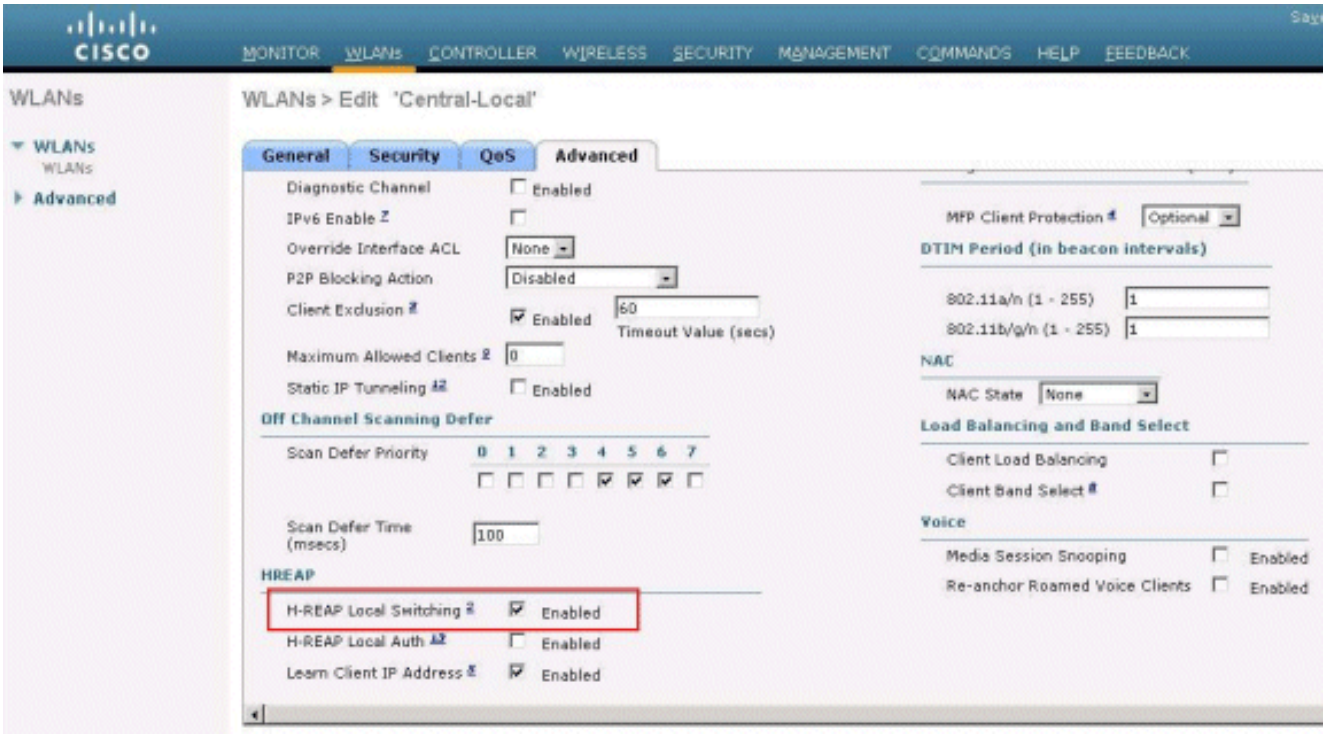
1. Clique **WLAN** a fim criar um Central-Local nomeado WLAN novo, a seguir clique-os **aplicam-se**.
2. Porque este WLAN usa a autenticação central, escolha a autenticação **WPA2 no** campo de Segurança da camada
   2.



3. Sob os servidores Radius secione, escolha o server apropriado configurado para a autenticação.



4. Verifique a caixa de verificação do **switching local H-REAP** a fim comutar o tráfego do cliente que pertence a este WLAN localmente no H-REAP.



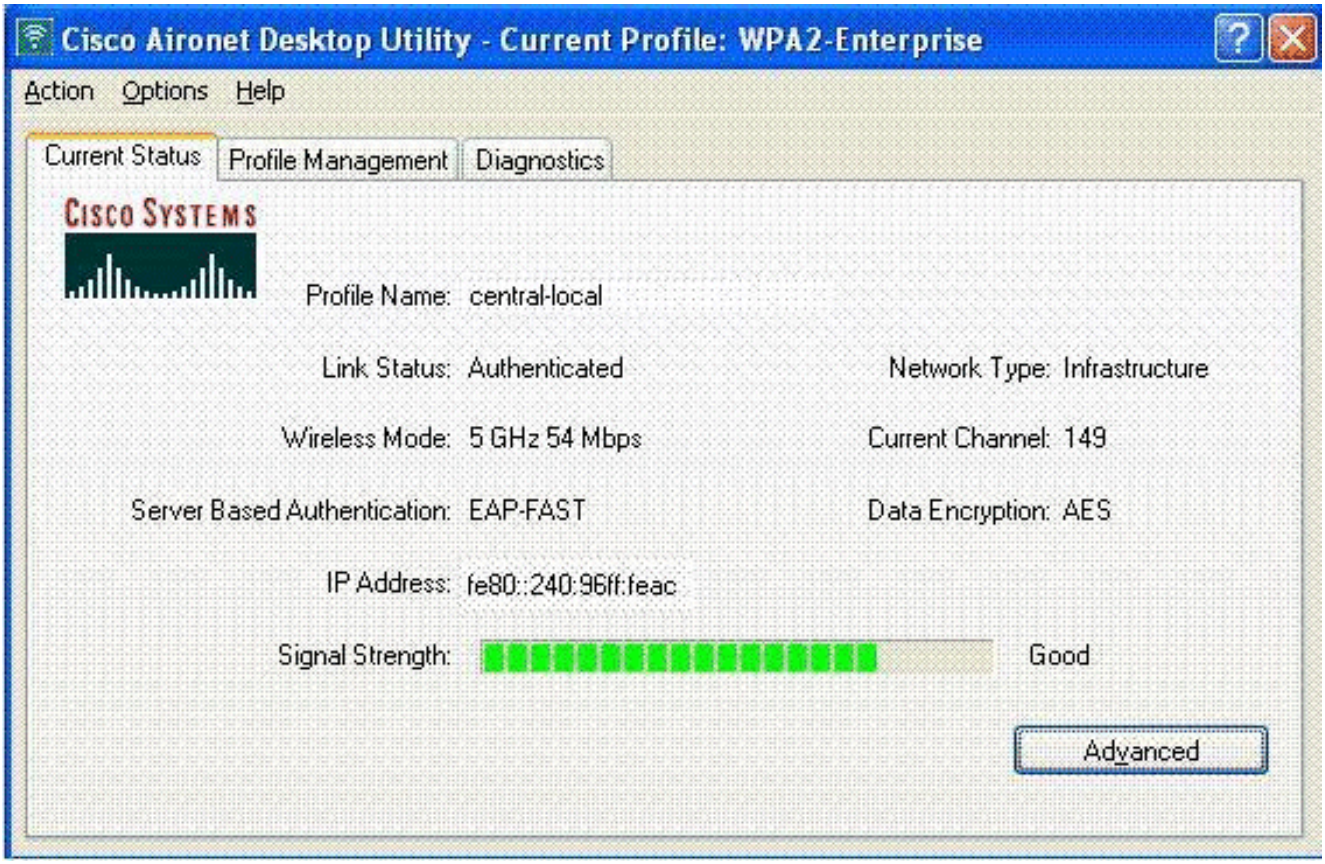
Verifique a autenticação central, switching local

Conclua estes passos:

1. Configurar o cliente Wireless com o mesmos SSID e configurações de segurança.Neste exemplo, o SSID é Central-*local* e o método de segurança é *WPA2*.
2. Incorpore o nome de usuário e senha como configurado no server>User do RAIO Setup a fim ativar o SSID central-local no cliente.Este exemplo usa o *usuário1* como o nome de usuário e

senha.
3. Clique em **OK**.O cliente centralmente é autenticado pelo servidor Radius e obtém associado com o H-REAP AP. O H-REAP está agora na **autenticação central, switching**

local.



Autenticação para baixo, switching local

Se um WLAN localmente comutado é configurado para qualquer tipo do autenticação que estiver exigido ser processado no WLC (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**. Neste estado, para o WLAN dado, o H-REAP rejeita todos os clientes novos que tentarem autenticar. Contudo, continua a enviar balizas e sondar respostas para manter clientes existentes conectados corretamente. Este estado é válido somente no modo independente.

A fim verificar este estado, use a mesma configuração explicada na autenticação central, seção de switching local.

Se o link MACILENTO que conecta o WLC está para baixo, o WLC atravessa o processo de cancelar a matrícula o H-REAP.

Uma vez que o registro desfeito/cancelado, H-REAP entra no modo independente.

O cliente associado com este WLAN ainda mantém sua Conectividade. Contudo, porque o controlador, o autenticador não está disponível, H-REAP não permite nenhuma novas conexões deste WLAN.

Isto pode ser verificado pela ativação de um outro cliente Wireless no mesmo WLAN. Você pode encontrar que a autenticação para este cliente falha e que não está permitido ao cliente associar.

Nota: Quando uma contagem do cliente de WLAN iguala zero, o H-REAP cessa todas as funções associadas do 802.11 e já não ilumina-as para o SSID dado. Isto abaixa o WLAN para o estado seguinte H-REAP, **autenticação, comutando para baixo**.

Autenticação local, switching local

Neste estado, o REGAÇO H-REAP segura authenticações do cliente 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 AP e não envolvem o processamento do controlador

O H-REAP que estava previamente na **autenticação central,** estado do **switching local**, movimentos neste estado, desde que o tipo do autenticação configurado pode ser segurado localmente no AP. Se a autenticação configurada não pode ser segurada localmente, como a autenticação do 802.1x, a seguir no modo independente, o H-REAP vai à **autenticação para baixo,** modo do **switching local**.

Estes são alguns dos mecanismos da autenticação populares que podem ser segurados localmente no AP no modo independente:

- Abrir
- Compartilhado
- WPA-PSK
- WPA2-PSK

Nota: Todos os processos de autenticação estão segurados pelo WLC quando o AP reage do modo conectado. Quando o H-REAP reagir do modo independente, aberto, compartilhado, e autenticações WPA/WPA2-PSK estão transferidos aos regaços onde toda a authenticação do cliente ocorre.

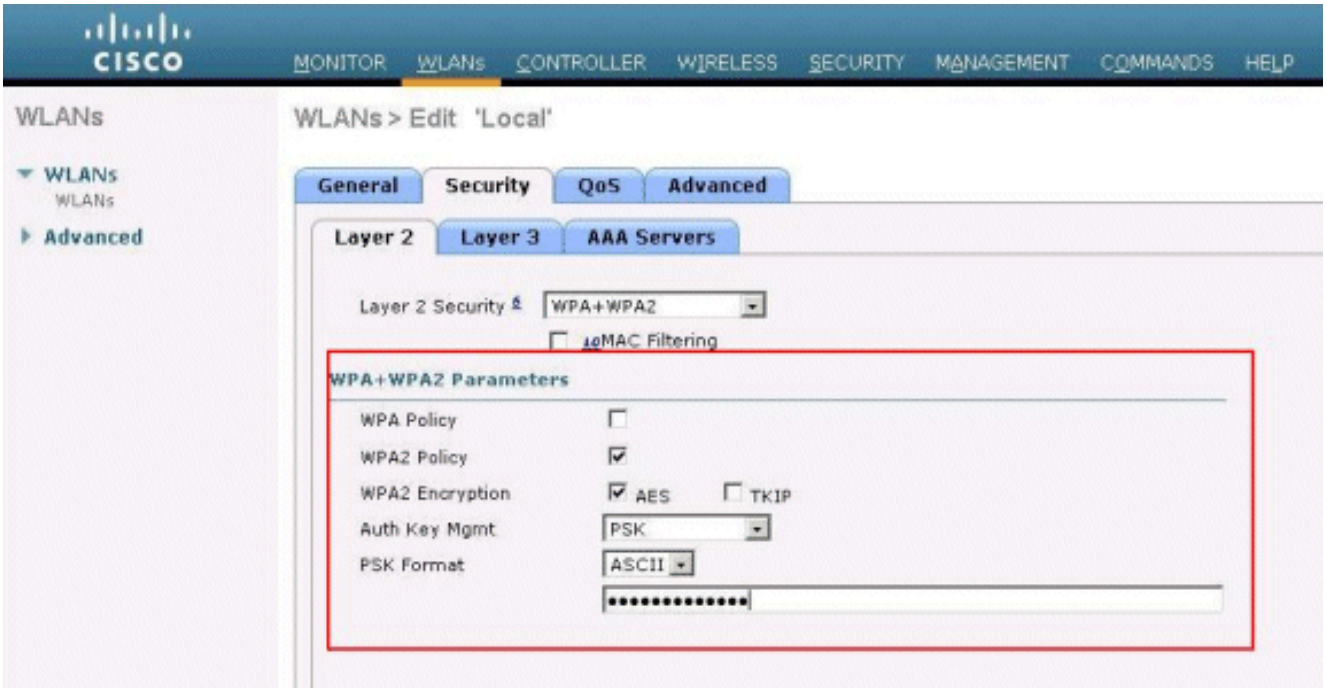
Nota: A autenticação do web externa não é apoiada ao se usar híbrido-COLHA com o switching local permitido no WLAN.

Este exemplo usa estes ajustes de configuração:

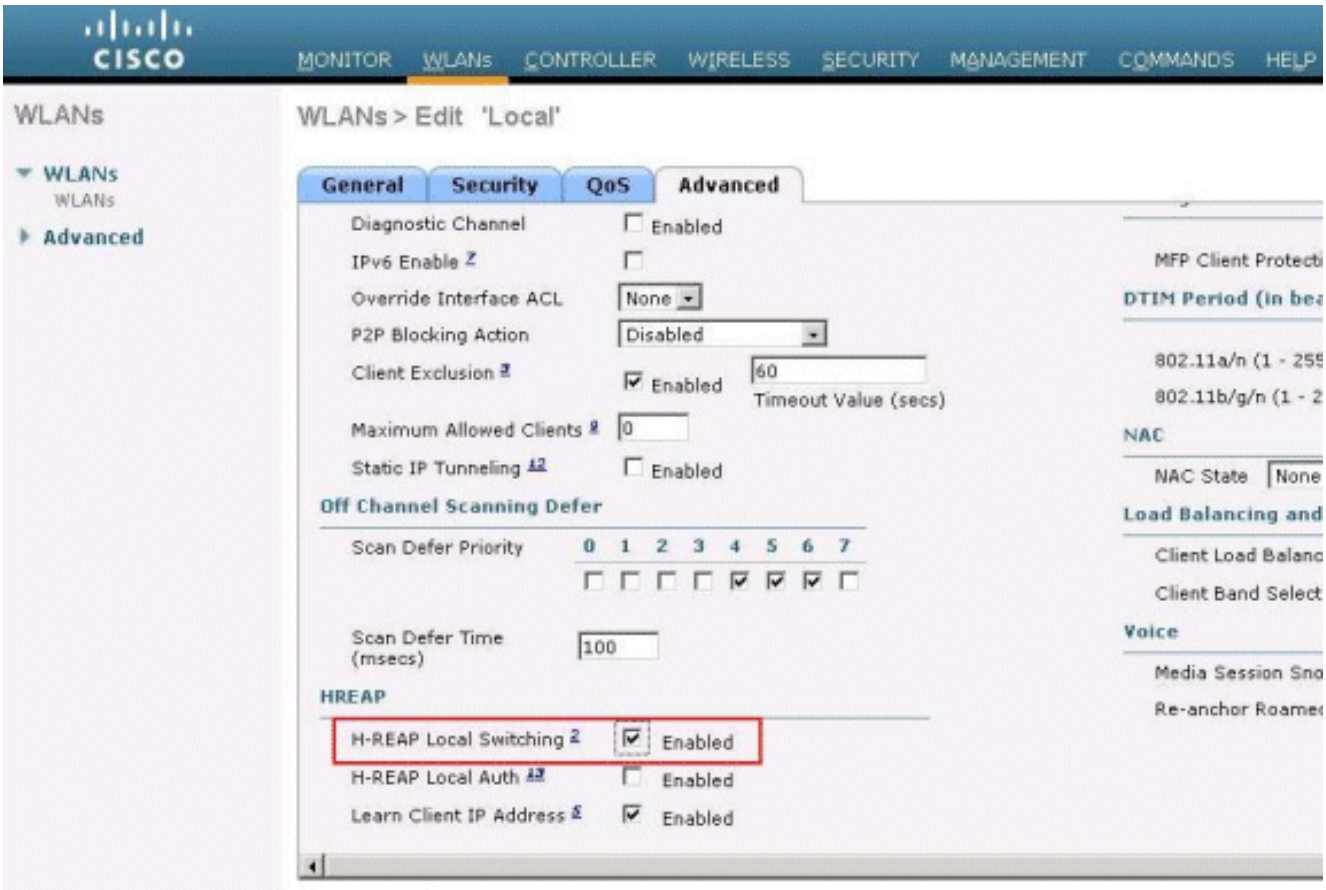
- Nome WLAN/SSID: **Local**
- Segurança da camada 2: **WPA-PSK**
- Switching local H-REAP: **habilitado**

Do controlador GUI, termine estas etapas:

1. Clique **WLAN** a fim criar um Local nomeado WLAN novo, a seguir clique-os **aplicam-se**.
2. Porque este WLAN usa a autenticação local, escolha o **WPA-PSK** ou o algum dos mecanismos de segurança mencionados que podem ser segurados localmente no campo de Segurança da camada 2.Este exemplo usa o **WPA-PSK**.



3. Uma vez que escolhido, você precisa de configurar a chave pré-compartilhada/frase de passagem a ser usada.Este deve ser o mesmo no lado do cliente para que a autenticação seja bem sucedida.
4. Verifique a caixa de verificação do **switching local H-REAP** a fim comutar o tráfego do cliente que pertence a este WLAN localmente no H-REAP.



Verifique a autenticação local, switching local

Conclua estes passos:

1. Configurar o cliente com o mesmos SSID e configurações de segurança.Aqui, o SSID é *local* e o método de segurança é *WPA-PSK*.
2. Ative o SSID local no cliente.O cliente obtém autenticado centralmente no controlador e associa com o H-REAP. O tráfego do cliente é configurado para comutar localmente. Agora, o H-REAP está na autenticação central, estado do switching local.
3. Desabilite o link MACILENTO que conecta ao controlador.O controlador atravessa como de costume o processo da cancelamento da matrícula. H-REAP é cancelado a matrícula do controlador.Uma vez que o registro desfeito/cancelado, H-REAP entra no modo independente.Contudo, o cliente que pertence a este WLAN ainda mantém a associação com H-REAP.Também, porque o tipo do autenticação aqui pode ser segurado localmente no AP sem o controlador, H-REAP permite associações de todo o cliente Wireless novo com este WLAN.
4. A fim verificar isto, ative todo o outro cliente Wireless no mesmo WLAN.Você pode ver que o cliente está autenticado e associado com sucesso.

Troubleshooting

- A fim pesquisar defeitos mais edições da conectividade de cliente na porta de Console do H-REAP, incorpore este comando:`AP_CLI#show capwap reap association`
- 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>`
- A fim debugar problemas de conectividade do 802.11 de um cliente, use este comando:`AP_CLI#debug dot11 state enable`
- Debugar o processo de autenticação e as falhas do 802.1X de um cliente com este comando:`AP_CLI#debug dot1x events enable`
- As mensagens backend controller/RADIUS podem ser debugadas usando este comando:`AP_CLI#debug aaa events enable`
- Alternativamente, para permitir um terno completo de **comandos debug do** cliente, use este comando:`AP_CLI#debug client <client's MAC address>`

Informações Relacionadas

- Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- VLAN no exemplo de configuração dos controladores do Wireless LAN
- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0
- O híbrido COLHE o projeto e o guia de distribuição
- Troubleshooting básico remoto híbrido do Access point da borda (H-REAP)
- Failover do controlador de WLAN para o exemplo de configuração do Lightweight Access Points
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems