Exemplo de Configuração dos Modos de Operação H-REAP

Contents

Introduction **Prerequisites Requirements** Componentes Utilizados Conventions Informações de Apoio H-REAP sobre REAP Configurar Diagrama de Rede Configuração Primando o AP com um controlador e configurando o H-REAP Teoria das operações H-REAP Estados de switching H-REAP Autenticação central, switching central Verificar a autenticação central, switching central Autenticação desativada, switching desativada Autenticação central, comutação local Verificar a autenticação central, comutação local Autenticação inativa, comutação local Autenticação local, comutação local Verificar a autenticação local, comutação local Troubleshoot Informações Relacionadas

Introduction

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.

Prerequisites

Requirements

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

Conhecimento dos Wireless LAN Controllers (WLCs) e como configurar os parâmetros

básicos da WLC

Conhecimento do REAP

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa o firmware versão 7.0.116.0
- Access Point Lightweight (LAP) Cisco 1131AG
- Cisco 2800 Series Routers que executam a versão 12.4(11)T.
- Adaptador de cliente Cisco Aironet 802.11a/b/g que executa o firmware versão 4.0
- Cisco Aironet Desktop Utility versão 4.0
- Cisco Secure ACS que executa a versão 4.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

O H-REAP é uma solução sem fio para implantações em filiais e escritórios remotos. O H-REAP permite que os clientes configurem e controlem access points (APs) em uma filial ou escritório remoto do escritório corporativo por meio de um link WAN sem implantar um controlador em cada escritório.

Os H-REAPs podem alternar o tráfego de dados de clientes localmente e executar a autenticação local do cliente quando a conexão com o 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 AP REAP híbrido também pode executar a autenticação local.

O H-REAP só é suportado em:

- APs 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040 e AP3550
- Controladores Cisco 5500, 4400, 2100, 2500 e Flex 7500 Series
- Switch de controlador integrado Catalyst 3750G
- Módulo de serviços sem fio (WiSM) Catalyst 6500 Series
- Módulo controlador de LAN sem fio (WLCM) para roteadores de serviços integrados (ISRs)

O tráfego do cliente em H-REAPs pode ser comutado localmente no AP ou tunelado de volta para um controlador. Isso depende da configuração por WLAN. Além disso, o tráfego de cliente comutado localmente no H-REAP pode ser marcado como 802.1Q para fornecer separação do lado com fio. Durante a interrupção da WAN, o serviço em todas as WLANs localmente comutadas e autenticadas localmente persiste.

Observação: se os APs estiverem no modo H-REAP e forem comutados localmente no local remoto, a atribuição dinâmica de usuários a uma VLAN específica com base na configuração do

servidor RADIUS não é suportada. No entanto, você deve ser capaz de atribuir usuários a VLANs específicas com base na VLAN estática para mapeamento de identificador de conjunto de serviços (SSID) feito localmente no AP. Portanto, um usuário que pertence a um SSID específico pode ser atribuído a uma VLAN específica para a qual o SSID é mapeado localmente no AP.

Observação: se voz sobre WLAN for importante, os APs devem ser executados no modo local para que obtenham suporte CCKM e Controle de Admissão de Conexão (CAC - Connection Admission Control), que não são suportados no modo H-REAP.

H-REAP sobre REAP

Consulte <u>Exemplo de Configuração de Remote-Edge AP (REAP) com APs Lightweight e</u> <u>Controladores Wireless LAN (WLCs)</u> para obter mais informações para ajudar a entender o REAP.

O H-REAP foi introduzido em resultado destas deficiências do REAP:

- O REAP não tem separação do lado da rede com fio. Isso se deve à falta de suporte para 802.1Q. Os dados das WLANs pousam na mesma sub-rede com fio.
- Durante uma falha de WAN, um AP REAP pára o serviço oferecido em todas as WLANs, exceto o primeiro especificado na controladora.

Éassim que o H-REAP supera essas duas deficiências:

- Fornece suporte dot1Q e mapeamento de VLAN para SSID. Esse mapeamento de VLAN para SSID precisa ser feito em H-REAP. Ao executar isso, certifique-se de que as VLANs configuradas sejam permitidas corretamente através das portas em switches e roteadores intermediários.
- Fornece serviço contínuo a todas as WLANs configuradas para comutação 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 pressupõe que o controlador já está configurado com configurações básicas. O controlador usa estas configurações:

- Endereço IP da interface de gerenciamento-172.16.1.10/16
- Endereço IP da interface do gerenciador de AP-172.16.1.11/16
- Endereço IP do roteador do gateway padrão-172.16.1.25/16
- Endereço IP do Virtual Gateway—1.1.1.1

Observação: este documento não mostra as configurações de WAN e a configuração de roteadores e switches disponíveis entre o H-REAP e o controlador. Isso pressupõe que você esteja ciente do encapsulamento da WAN e dos protocolos de roteamento usados. Além disso, este documento pressupõe que você entenda como configurá-los para manter a conectividade entre o H-REAP e o controlador através do link da WAN. Neste exemplo, o encapsulamento HDLC é usado no link da WAN.

Primando o AP com um controlador e configurando o H-REAP

Se você quiser que o AP descubra um controlador de uma rede remota onde os mecanismos de descoberta CAPWAP não estejam disponíveis, você pode usar a preparação. Esse método permite especificar a controladora à qual o AP deve se conectar.

Para preparar um AP com capacidade para H-REAP, conecte o AP à rede com fio no escritório central. Durante a inicialização, o AP com capacidade para H-REAP primeiro procura um endereço IP para si mesmo. Depois de adquirir um endereço IP através de um servidor DHCP, ele é inicializado e procura um controlador para executar o processo de registro.

Um AP H-REAP pode aprender o endereço IP da controladora de qualquer uma das maneiras explicadas no registro LAP (Lightweight AP) em uma WLC (Wireless LAN Controller, Controladora de LAN Wireless).

Observação: você também pode configurar o LAP para descobrir o controlador através dos comandos CLI no AP. Consulte <u>Descoberta do controlador H-REAP usando comandos CLI</u> para obter mais informações.

O exemplo neste documento usa o procedimento da opção 43 do DHCP para o H-REAP aprender o endereço IP do controlador. Em seguida, ele se junta ao controlador, faz o download da imagem e da configuração de software mais recentes do controlador e inicializa o link de rádio. Ele salva a configuração baixada na memória não volátil para uso no modo autônomo.

Quando o LAP estiver registrado na controladora, faça o seguinte:

- 1. Na GUI do controlador, escolha **Wireless>Access Points**.Exibe o LAP registrado com este controlador.
- 2. Clique no AP que deseja

configurar.	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	Sa <u>v</u> e Con
Wireless	All APs			notio - London p.	2014/2021 142	ilonokkino.	2224	1996 - 1995 - 1995 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 -	
 Access Points All APs Radios 802.11a/n 802.11b/g/n Global Configuration 	Current Filter		Norhe 1		[Change Filter]	[Clear Filter]			
Advanced	AP Name	AP Mod	el		P MAC	AP Up Tin	ne	Admin Status	Operational Status
HREAP Groups	AP001a.a219.ad44	AIR-LAP	1131AG-A-K9		00:1a:a2:19:ad:44	0 d, 00 h 0	6 m 12 s	Enabled	REG
▶ 802.11a/n ▶ 802.11b/n/n									

3. Na janela APs>Detalhes, clique na guia Alta disponibilidade e defina os nomes de controlador que os APs usarão para registrar-se e clique em

		2		-	
А	n	L	ся	r	
/ \			uu		

ll. cisco	MONITOR WLANS CO		SS <u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Wireless	All APs > Details for A	AP001a.a219.ad44					
 Access Points All APs Radios 802.11a/n 802.11b/g/n Global Configuration Advanced Mesh HREAP Groups 802.11a/n 802.11b/g/n B02.11b/g/n B02.	General Credentia Primary Controller Secondary Controller Tertiary Controller AP Failover Priority	Name WLC-4400	High Availability Manager 172.1	Inventory gement IP Addre	Advanced		
Country Timers > QoS							

Você pode definir até três nomes de controlador (principal, secundário e terciário). Os APs pesquisam o controlador na mesma ordem que você fornece nessa janela. Como este exemplo usa apenas um controlador, o exemplo define o controlador como o controlador principal.

4. Configure o LAP para H-REAP.Para configurar o LAP para operar no modo H-REAP, na janela APs>Detalhes, na guia Geral, escolha o **modo AP** como H-REAP no menu suspenso correspondente.Isso configura o LAP para operar no modo H-

/ireless	General Credential	s Interfaces High Availabilit	y Inventory Advanced	
Access Points	General		Versions	
Radios	AP Name	AP001a.a219.ad44	Primary Software Version	7.0.116.0
802.11b/g/n	Location	default location	Backup Software Version	0.0.0.0
Global Configuration	AP MAC Address	00:1a:a2:19:ad:44	Predownload Status	None
Advanced	Base Radio MAC	00:1a:30:c0:e3:50	Predownloaded Version	None
Mesh	Admin Status	Enable .	Predownload Next Retry Time	NA NA
HREAP Groups	AP Mode	H-REAP .	Predownload Retry Count	NA
802.11a/n	AP Sub Mode	local	Boot Version	12.3.8.0
802.11b/g/n	Operational Status	monitor	10S Version	12.4(23c)3A2
Media Stream	Port Number	Sniffer	Mini 105 Version	3.0.51.0
Country		Bridge	IP Config	
Timers			IP Address	10.78.177.28
Qe5			Static IP	9
			Static IP 172.1	8.1.10
			Netmask 255.2	55.0.0
			Gateway 17.18	.1.25
			A DNS IP Address 0.0.0.	0
			Domain Name	

Observação: neste exemplo, você pode ver que o endereço IP do AP é alterado para o modo estático e o endereço IP estático 172.18.1.10 foi atribuído. Esta atribuição ocorre porque esta é a sub-rede a ser usada no escritório remoto. Portanto, você usa o endereço IP do servidor DHCP, mas somente durante a primeira etapa do registro. Depois que o AP for

registrado no controlador, você alterará o endereço para um endereço IP estático. Agora que o LAP está ativado com o controlador e configurado para o modo H-REAP, a próxima etapa é configurar o H-REAP no lado do controlador e discutir os estados de switching do H-REAP.

Teoria das operações H-REAP

O LAP compativel com H-REAP opera nestes dois modos diferentes:

- Modo conectado: Diz-se que um H-REAP está no modo conectado quando o link do plano de controle CAPWAP para a WLC está ativo e operacional. Isso significa que o link da WAN entre o LAP e a WLC não está inoperante.
- Modo autônomo: Diz-se que um H-REAP está no modo autônomo quando seu link de WAN para a WLC está inoperante. Por exemplo, quando esse H-REAP não tem mais conectividade com a WLC conectada pelo link da WAN.

O mecanismo de autenticação usado para autenticar um cliente pode ser definido como **Central** ou **Local**.

- Autenticação central—Refere-se ao tipo de autenticação que envolve o processo da WLC a partir do local remoto.
- Autenticação local—Refere-se aos tipos de autenticação que não envolvem nenhum processamento do WLC para autenticação.

Observação: todo o processamento de autenticação e associação do 802.11 ocorre no H-REAP, independentemente do modo em que o LAP está. No modo conectado, o H-REAP faz o proxy dessas associações e autenticações para a WLC. No modo autônomo, o LAP não pode informar a WLC sobre tais eventos.

Quando um cliente se conecta a um AP H-REAP, o AP encaminha todas as mensagens de autenticação para o controlador. Após a autenticação bem-sucedida, seus pacotes de dados são comutados localmente ou encapsulados de volta para o controlador. Isso está de acordo com a configuração da WLAN à qual ela está conectada.

Com o H-REAP, as WLANs configuradas em um controlador podem ser operadas em dois modos diferentes:

- **Comutação central:**Diz-se que uma WLAN em H-REAP opera no modo de comutação central se o tráfego de dados dessa WLAN estiver configurado para ser encapsulado na WLC.
- Switching local:Diz-se que uma WLAN em H-REAP opera no modo de comutação local se o tráfego de dados dessa WLAN termina localmente na interface com fio do próprio LAP, sem ser encapsulado na WLC.Observação: somente as WLANs de 1 a 8 podem ser configuradas para switching local H-REAP porque somente essas WLANs podem ser aplicadas aos APs das séries 1130, 1240 e 1250 que suportam a funcionalidade H-REAP.

Estados de switching H-REAP

Combinado com os modos de autenticação e comutação mencionados na seção anterior, um H-REAP pode operar em qualquer um destes estados:

• Autenticação central, switching central

- <u>Autenticação desativada, switching desativada</u>
- <u>Autenticação central, comutação local</u>
- <u>Autenticação inativa, comutação local</u>
- <u>Autenticação local, comutação local</u>

Autenticação central, switching central

Nesse estado, para a WLAN fornecida, o AP encaminha todas as solicitações de autenticação de cliente ao controlador e encaminha todos os dados de cliente para a WLC. Esse estado é válido somente quando o H-REAP está no modo conectado. Qualquer WLAN configurada para operar nesse modo é perdida durante uma falha de WAN, independentemente do método de autenticação.

Este exemplo usa estas configurações:

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

Conclua estes passos para configurar a WLC para autenticação central, comutação central usando GUI:

1. Clique em WLANs para criar uma nova WLAN chamada Central e clique em

|--|

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs	WLANs > New	WLAN	-					
Advanced	Profile Name SSID ID	Centr. Centr.	al al					

 Como essa WLAN usa autenticação central, usamos a autenticação WPA2 no campo Layer
 Security. A WPA2 é a segurança de camada 2 padrão para uma WLAN.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANS WLANS WLANS Advanced	WLANS > Edit 'Central' General Security QoS Advanced Profile Name Central Type WLAN SSID Central Status Image: Enabled Security Policies [WPA2][Auth(802.1%)] Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) management Imagement Ima

3. Escolha a guia Servidores AAA e escolha o servidor apropriado configurado para autenticação.

CISCO	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT CO	MMANDS HELP <u>F</u> EED84
_ANs	WLANs > Edit 'Central'		
WLANS WLANS	General Security QoS /	Advanced	
Advanced	Layer 2 Layer 3 AAA Ser	vers	
	Server 1 Server 2	Authentication Servers Accounting Server Enabled None None None None None None None None	Server 2 None • Server 3 None •
	Server 3	None None -	
	Local EAP Authentication		
	Authentication priority order for web-auth user	bled Dr	
	4 ···· ·		

 Como esta WLAN usa comutação central, você precisa garantir que a caixa de seleção Comutação local H-REAP esteja desabilitada (ou seja, a caixa de seleção Comutação local não está selecionada). Em seguida, clique em Aplicar.

LANs	WLANs > Edit 'Central'	
WLANS WLANS Advanced	General Security QoS Advanced Diagnostic Channel Enabled IPv6 Enable 2 Enabled Override Interface ACL None • P2P Blocking Action Disabled Client Exclusion 2 Imabled Maximum Allowed Clients 2 Imabled Static IP Tunneling 42 Enabled Off Channel Scanning Defer Imabled Scan Defer Priority 0 1 2 3 4 5 7	MFP Client Protection d Optional DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 NAC NAC State None Lead Balancing and Band Select Client Load Balancing Client Band Select f
	Scan Defer Time (Insecs) HREAP H-REAP Local Switching R Enabled H-REAP Local Auth R Enabled Learn Client IP Address R Enabled	Voice Media Session Snooping 🔲 Enabled Re-anchor Roamed Voice Clients 🗖 Enabled

Verificar a autenticação central, switching central

Conclua estes passos:

- 1. Configure o cliente sem fio com o mesmo SSID e as mesmas configurações de segurança.Neste exemplo, o SSID é *Central* e o método de segurança é *WPA2*.
- 2. Insira o nome de usuário e a senha configurados no servidor RADIUS>User Setup para ativar o SSID central no cliente.Este exemplo usa *User1* como nome de usuário e

network	Ar 1 Ao 1 userhame and password to log on to the wroless
User Name :	User1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name :	WPA-Enterprise

é autenticado centralmente pelo servidor RADIUS e está associado ao AP H-REAP. O H-REAP está agora na **autenticação central, comutação central**.

🛜 Cisco Aironet Desktop	Utility - Current Profile:	WPA2-Enterprise
Action Options Help		
Current Status Profile Mana	gement Diagnostics	
UILIUUUILIUU Profile	Name: central	
Link	Status: Authenticated	Network Type: Infrastructure
Wireles	s Mode: 5 GHz 54 Mbps	Current Channel: 149
Server Based Authen	tication: EAP-FAST	Data Encryption: AES
IPA	ddress: fe80::240:96ff:feac	
Signal S	trength:	Good
		Advanced

Autenticação desativada, switching desativada

Com a mesma configuração explicada na seção <u>Central Authentication, Central Switching</u>, desative o link da WAN que conecta o controlador. Agora, o controlador espera uma resposta de pulsação do AP. Uma resposta de pulsação é semelhante a mensagens de keepalive. O controlador tenta cinco batimentos de coração consecutivos, a cada segundo.

Como não é recebido com uma resposta de pulsação do H-REAP, a WLC anuncia o registro do LAP.

Execute o comando **debug capwap events enable** na CLI da WLC para verificar o processo de cancelamento de registro. Este é o exemplo de saída 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 autônomo.

Como essa WLAN era previamente autenticada centralmente e comutada centralmente, tanto o tráfego de controle quanto o de dados eram enviados ao túnel para o controlador. Portanto, sem o controlador, o cliente não consegue manter a associação com o H-REAP e é desconectado. Esse estado de H-REAP com associação de cliente e autenticação inoperante é conhecido como Authentication Down (Autenticação inativa), Switching Down (Desativação da autenticação).

Autenticação central, comutação local

Nesse estado, para a WLAN fornecida, a WLC lida com toda a autenticação do cliente e o LAP H-REAP comuta os pacotes de dados localmente. Depois que o cliente se autentica com êxito, o controlador envia comandos de controle capwap ao H-REAP e instrui o LAP a comutar os pacotes de dados do cliente. Esta mensagem é enviada por cliente na autenticação bem-sucedida. Esse estado é aplicável somente no modo conectado.

Este exemplo usa estas configurações:

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

Na GUI do controlador, faça o seguinte:

- 1. Clique em WLANs para criar uma nova WLAN chamada Central-Local e clique em Aplicar.
- 2. Como essa WLAN usa autenticação central, escolha a autenticação WPA2 no campo Layer 2

WLANs	WLANs > Edit 'Central-Local'
 WLANS WLANS ▶ Advanced 	General Security QoS Advanced Profile Name Central-Local Type WLAN SSID Central-Local Status Image: Enabled
	Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) management * Multicast Vian Feature Enabled Broadcast SSID Fenabled

3. Na seção Servidores Radius, escolha o servidor apropriado configurado para autenticação.

cisco		OLLER WIRELESS SECURITY	MANAGEMENT COM	MANDS HELP EEEDBACK
WLANs	WLANs > Edit 'Central-L	ocal'		
WLANS WLANS	General Security Q	oS Advanced		
▶ Advanced	Layer 2 Layer 3	AAA Servers		
	Radius Servers Radius Server Overwrite	interface C Enabled Authentication Servers	Accounting Servers	Server 1 None - Server 2 None -
		Enabled	Enabled	Server 3 None -
	Server 1	None	None -	
	Server 2	None IP:172.16.1.1, Port:1812	None •	
	Server 3	None	None +	
	Local EAP Authentication	5		
	Local EAP Authentication Authentication priority web-auth user	order for	11 12 12	

 Marque a caixa de seleção H-REAP Local Switching para alternar o tráfego do cliente que pertence a esta WLAN localmente no H-REAP

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	Sa C <u>o</u> mmands Help <u>F</u> eedback
WLANS WLANS WLANS Advanced	WLANS > Edit "Central-Local" General Security QoS Advanced Diagnostic Channel Enabled IPv6 Enable Z Image: Control of the second seco	MFP Client Protection # Optional DTIM Period (in beacon intervals) S02.11a/h (1 - 255) 1 S02.11b/g/h (1 - 255) 1 NAC NAC State None Load Balancing and Band Select Client Load Balancing Client Band Select # Voice Media Session Snooping Re-anchor Roamed Voice Clients □ Enabled

Verificar a autenticação central, comutação local

Conclua estes passos:

- 1. Configure o cliente sem fio com o mesmo SSID e as mesmas configurações de segurança.Neste exemplo, o SSID é *Central-Local* e o método de segurança é *WPA2*.
- 2. Insira o nome de usuário e a senha configurados no servidor RADIUS>User Setup para ativar o SSID local-central no cliente.Este exemplo usa *User1* como nome de usuário e

network	
Jser Name :	User1
Password :	•••••
.og on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
DesGle Massa -	11/PA Enterprise

senha.

 Click OK.O cliente é autenticado centralmente pelo servidor RADIUS e é associado ao AP H-REAP. O H-REAP está agora na autenticação central, comutação local.

Cisco Airon	et Desktop Utility	y - Current Profile	: WPA2-Enterprise	? 🔀
Action Options	Help			
Current Status	Profile Management	Diagnostics		
ահրատի	In Profile Name:	central-local		
	Link Status:	Authenticated	Network Type: Infrastructur	e
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server B	ased Authentication:	EAP-FAST	Data Encryption: AES	
	IP Address:	fe80::240:96ff:feac		
	Signal Strength:		Good	
			Advanced	

Autenticação inativa, comutação local

Se uma WLAN comutada localmente estiver configurada para qualquer tipo de autenticação que seja necessário processar na WLC (como a autenticação EAP [WEP/WPA/WPA2/802.11i], WebAuth ou NAC), em caso de falha na WAN, ela entra no estado **de falha de autenticação**,

switching local. Nesse estado, para a WLAN fornecida, o H-REAP rejeita qualquer novo cliente que tente autenticar. No entanto, ele continua a enviar beacons e respostas de sondagem para manter os clientes atuais conectados corretamente. Esse estado é válido somente no modo autônomo.

Para verificar esse estado, use a mesma configuração explicada na seção <u>Autenticação Central,</u> <u>Comutação Local</u>.

Se o link da WAN que conecta a WLC estiver inoperante, a WLC passará pelo processo de cancelamento de registro do H-REAP.

Depois de cancelar o registro, o H-REAP entra no modo autônomo.

O cliente associado por meio desta WLAN ainda mantém sua conectividade. No entanto, como o controlador, o autenticador não está disponível, o H-REAP não permite novas conexões desta WLAN.

Isso pode ser verificado pela ativação de outro cliente sem fio na mesma WLAN. Você pode descobrir que a autenticação para este cliente falha e que ele não tem permissão para se associar.

Observação: quando uma contagem de clientes WLAN é igual a zero, o H-REAP cessa todas as funções 802.11 associadas e não mais sinalizadores para o SSID especificado. Isso move a WLAN para o próximo estado H-REAP, **autenticação desativada, alternando para baixo**.

Autenticação local, comutação local

Nesse estado, o LAP H-REAP lida com as autenticações do cliente e comuta os pacotes de dados do cliente localmente. Esse estado é válido somente no modo autônomo e somente para tipos de autenticação que podem ser tratados localmente no AP e não envolvem o processamento do controlador

O H-REAP que estava anteriormente na **autenticação central, no** estado de **comutação local**, move-se para este estado, desde que o tipo de autenticação configurado possa ser manipulado localmente no AP. Se a autenticação configurada não puder ser tratada localmente, como a autenticação 802.1x, então no modo autônomo, o H-REAP vai para a **autenticação desativada, o** modo **de comutação local**.

Estes são alguns dos mecanismos de autenticação populares que podem ser manipulados localmente no AP no modo autônomo:

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

Observação: todos os processos de autenticação são tratados pela WLC quando o AP está no modo conectado. Enquanto o H-REAP está no modo autônomo, as autenticações de WPA/WPA2-PSK, abertas, compartilhadas e abertas são transferidas para os LAPs onde ocorre toda a autenticação de cliente.

Observação: a autenticação externa da Web não é suportada ao usar o REAP híbrido com a comutação local habilitada na WLAN.

Este exemplo usa estas configurações:

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

Na GUI do controlador, faça o seguinte:

- 1. Clique em WLANs para criar uma nova WLAN chamada Local e clique em Aplicar.
- Como essa WLAN usa autenticação local, escolha WPA-PSK ou qualquer um dos mecanismos de segurança mencionados que podem ser tratados localmente no campo Segurança da Camada 2.Este exemplo usa WPA-PSK

cisco	MONITOR WLANS CON	ITROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit 'Local'	n National Constant Constant (Constant) Constant Constant (Constant) Constant (Constant) National Constant (Constant)
WLANS WLANS	General Security	QoS Advanced
▶ Advanced	Layer 2 Layer 3	AAA Servers
	WPA+WPA2 Parameter	's
	WPA Policy	
	WPA2 Policy	v
	WPA2 Encryption	AES TIMP
	Auth Key Mgmt	PSK
	PSK Format	ASCII -

- Depois de selecionado, você precisa configurar a Frase de chave/senha pré-compartilhada a ser usada.lsso deve ser o mesmo no lado do cliente para que a autenticação seja bemsucedida.
- Marque a caixa de seleção H-REAP Local Switching para alternar o tráfego do cliente que pertence a esta WLAN localmente no H-REAP.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	r c <u>o</u> mmands help
WLANS WLANS MLANS Advanced	WLANS > Edit 'Local' General Security QoS Advanced Diagnostic Channel IPv6 Enable Z Override Interface ACL None I P2P Blocking Action Disabled Client Exclusion I Waximum Allowed Clients I O Static IP Tunneling II Enabled Off Channel Scanning Defer Scan Defer Priority IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	MFP Client Protect DTIM Period (in be 802.11a/n (1 - 25 802.11b/g/n (1 - 3 NAC NAC State None Load Balancing and Client Load Balanc Client Band Select Voice Media Session Sn Re-anchor Roame

Verificar a autenticação local, comutação local

Conclua estes passos:

- 1. Configure o cliente com o mesmo SSID e as mesmas configurações de segurança.Aqui, o SSID é *Local* e o método de segurança é *WPA-PSK*.
- Ative o SSID local no cliente.O cliente é autenticado centralmente no controlador e se associa ao H-REAP. O tráfego do cliente é configurado para comutar localmente. Agora, o H-REAP está no estado de autenticação central, comutação local.
- 3. Desative o link da WAN que se conecta ao controlador.O controlador, como de costume, passa pelo processo de cancelamento de registro. O H-REAP é removido do registro da controladora.Depois de cancelar o registro, o H-REAP entra no modo autônomo.No entanto, o cliente que pertence a esta WLAN ainda mantém a associação com H-REAP.Além disso, como o tipo de autenticação aqui pode ser manipulado localmente no AP sem o controlador, o H-REAP permite associações de qualquer novo cliente sem fio através desta WLAN.
- 4. Para verificar isso, ative qualquer outro cliente sem fio na mesma WLAN.Você pode ver que o cliente foi autenticado e associado com êxito.

Troubleshoot

 Para solucionar problemas de conectividade do cliente na porta de console do H-REAP, insira este comando:

 $\texttt{AP_CLI}\#\texttt{show}$ capwap reap association

• Para solucionar problemas de conectividade do cliente no controlador e limitar a saída de mais depuração, use este comando:

- Para depurar os problemas de conectividade 802.11 de um cliente, use este comando: AP_CLI#debug dot11 state enable
- Depurar o processo de autenticação 802.1X de um cliente e as falhas com este comando: AP_CLI#debug dot1x events enable
- As mensagens de controlador de back-end/RADIUS podem ser depuradas usando este comando: AP_CLI#debug aaa events enable
- Como alternativa, para ativar um conjunto completo de comandos debug do cliente, use este comando:

AP_CLI#debug client

Informações Relacionadas

- Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight
- <u>VLANs no exemplo de configuração de Wireless LAN Controllers</u>
- Guia de configuração de Cisco Wireless LAN Controller, versão 7.0
- Guia de projeto e implantação do REAP híbrido
- Solução básica de problemas do H-REAP (Hybrid Remote Edge Access Point)
- Exemplo de Configuração de Failover do Controlador WLAN para Pontos de Acesso Lightweight
- <u>Suporte de produtos Wireless</u>
- <u>Suporte Técnico e Documentação Cisco Systems</u>