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

Contents

Introduction

Os recursos de ponto de acesso de borda remota (REAP) introduzidos com a Cisco Unified Wireless Network permitem a implantação remota dos Pontos de Acesso Lightweight (LAPs - Lightweight Access Points) da controladora de LAN sem fio (WLAN - Wireless LAN Controller). Isso os torna ideais para filiais e pequenos locais de varejo. Este documento explica como implementa uma rede WLAN com base em REAP com uso do Cisco 1030 Series LAP e do 4400 WLCs.

Prerequisites

Requirements

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

- Conhecimento das WLCs e como configurar os parâmetros básicos da WLC
- Conhecimento do modo de operação REAP em um LAP Cisco 1030
- Conhecimento da configuração de um servidor DHCP externo e/ou de um servidor DNS

(Domain Name System)
- Conhecimento dos conceitos de WPA (Wi-Fi Protected Access)

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa o firmware versão 4.2
- LAP Cisco 1030
- Dois Cisco 2800 Series Routers que executam o Cisco IOS® Software Release 12.2(13)T13
- Adaptador de cliente Cisco Aironet 802.11a/b/g que executa o firmware versão 3.0
- Cisco Aironet Desktop Utility versão 3.0

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

Informações de Apoio

O modo REAP permite que um LAP resida em um link WAN e ainda possa se comunicar com a WLC e fornecer a funcionalidade de um LAP regular. O modo REAP é suportado somente nos LAPs 1030 neste momento.

Para fornecer essa funcionalidade, o REAP 1030 separa o plano de controle LWAPP (Lightweight Access Point Protocol) do plano de dados sem fio. As WLCs da Cisco ainda são usadas para controle e gerenciamento centralizados da mesma forma que os APs (Access Points, pontos de acesso) baseados em LWAPP regulares são usados, enquanto todos os dados do usuário são interligados localmente no AP. O acesso aos recursos da rede local é mantido em todas as interrupções da WAN.

Os APs REAP suportam dois modos de operação:

- modo de REAP normal
- Modo autônomo

O LAP é definido no modo REAP normal quando o link WAN entre o REAP AP e a WLC está ativo. Quando os LAPs operam no modo REAP normal, eles podem suportar até 16 WLANs.

Quando o link da WAN entre a WLC e o LAP é desativado, o LAP ativado por REAP muda para o modo autônomo. No modo autônomo, os LAPs REAP podem suportar somente uma WLAN independentemente sem a WLC, se a WLAN estiver configurada com WEP (Wired Equivalent Privacy) ou qualquer método de autenticação local. Nesse caso, a WLAN que o AP REAP suporta é a primeira WLAN configurada no AP, WLAN 1. Isso ocorre porque a maioria dos outros métodos de autenticação precisa passar informações para e do controlador e, quando o link da WAN está inoperante, essa operação não é possível. No modo autônomo, os LAPs suportam um conjunto mínimo de recursos. Esta tabela mostra o conjunto de recursos que um LAP REAP suporta quando está no modo autônomo em comparação com os recursos que um LAP REAP suporta no

modo normal (quando o link WAN está ativo e a comunicação com a WLC está ativa):

Recursos que um REAP LAP suporta no modo REAP normal e no modo autônomo

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

A tabela mostra que várias VLANs não são suportadas em LAPs REAP em ambos os modos. Várias VLANs não são suportadas porque os LAPs REAP só podem residir em uma única sub-rede porque não podem executar a marcação de VLAN IEEE 802.1Q. Portanto, o tráfego em cada um dos SSIDs termina na mesma sub-rede da rede com fio. Como resultado, o tráfego de dados não é separado no lado com fio, mesmo que o tráfego sem fio possa ser segmentado no ar entre SSIDs.

Consulte o Guia de implantação do REAP na filial para obter mais informações sobre a

implantação do REAP e sobre como gerenciar o REAP e suas limitações.

Configurar

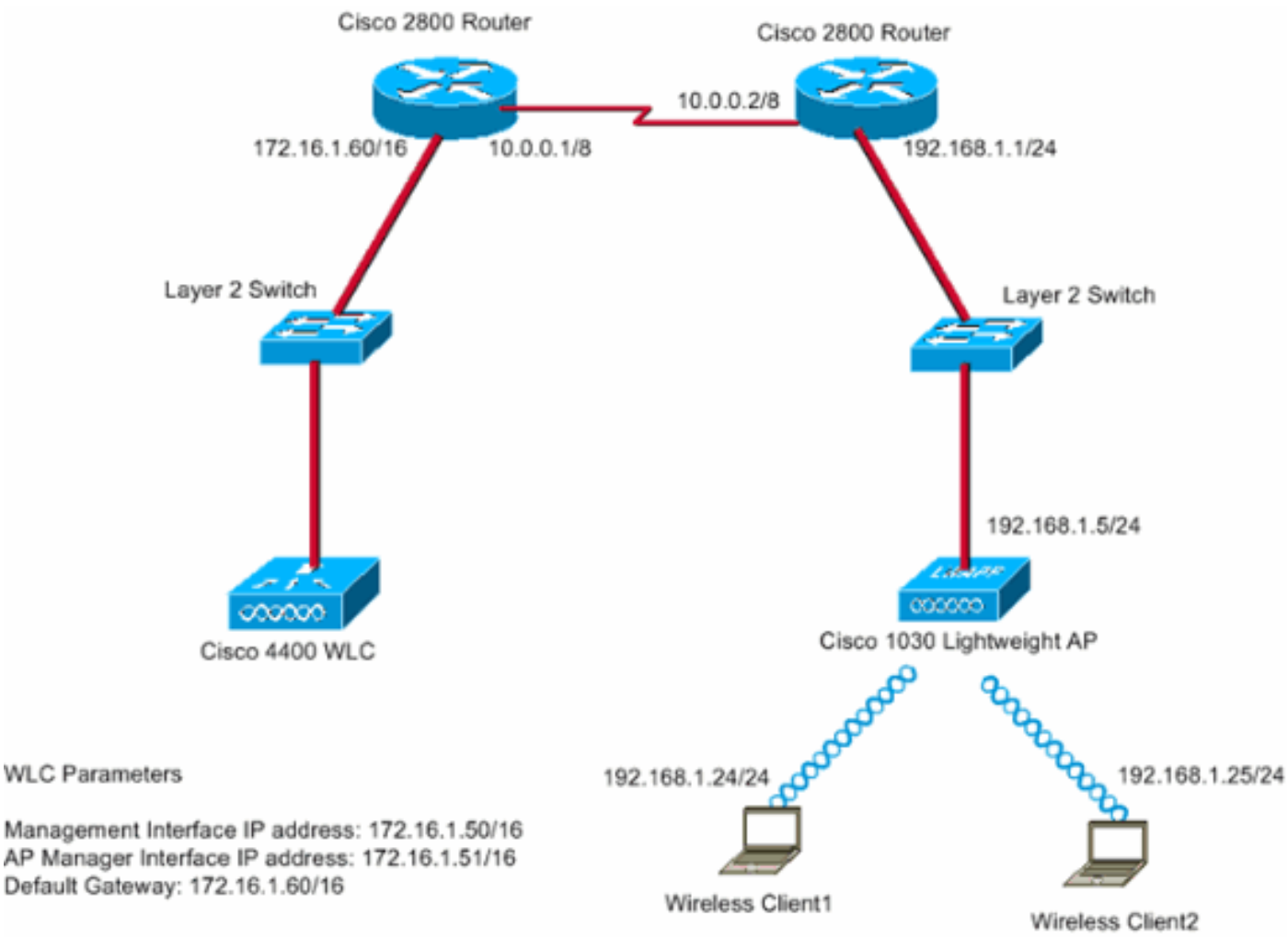
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Para configurar os dispositivos para implementar a configuração de rede, faça o seguinte:

1. Configure a WLC para operação básica e configure as WLANs.
2. Prima o AP para instalação no local remoto.
3. Configure os roteadores 2800 para estabelecer o link WAN.
4. Implante o LAP do REAP no local remoto.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



O escritório central se conecta à filial com o uso de uma linha alugada. A linha alugada termina em 2800 Series Routers em cada extremidade. Este exemplo usa o protocolo OSPF (Open Shortest Path First) para rotear dados no link da WAN com o encapsulamento PPP. A WLC 4400 está no escritório principal e o LAP 1030 deve ser implantado no escritório remoto. O LAP 1030 deve suportar duas WLANs. Aqui estão os parâmetros para as WLANs:

- **WLAN 1**SSID—**SSID1**Autenticação—**Aberta**Criptografia—**Temporal Key Integrity Protocol (TKIP) (WPA Pre-Shared Key [WPA-PSK])**
- **WLAN 2**SSID—**SSID2**Autenticação—**Extensible Authentication Protocol (EAP)**Criptografia—**TKIPObservação:** para a WLAN 2, a configuração neste documento usa WPA (autenticação 802.1x e TKIP para criptografia).

Você deve configurar os dispositivos para esta configuração.

Configurar o WLC para a operação básica e configurar as WLANs

Você pode usar o assistente de configuração de inicialização na interface de linha de comando (CLI) para configurar a WLC para a operação básica. Como alternativa, você também pode usar a GUI para configurar a WLC. Este documento explica a configuração no WLC com o uso do assistente de configuração de inicialização no CLI.

Depois que a WLC é inicializada pela primeira vez, ela entra diretamente no assistente de configuração de inicialização. Você usa o assistente de configuração para definir as configurações básicas. Você pode executar o assistente na CLI ou na GUI. Aqui está um exemplo do assistente de configuração de inicialização:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 172.16.1.60
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
AP Manager Interface IP Address: 172.16.1.51
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Main
Network Name (SSID): SSID1
Allow Static IP Addresses [YES][no]: Yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: Yes
Enable 802.11a Network [YES][no]: Yes
Enable 802.11g Network [YES][no]: Yes
Enable Auto-RF [YES][no]: Yes

Configuration saved!
Resetting system with new configuration...
```

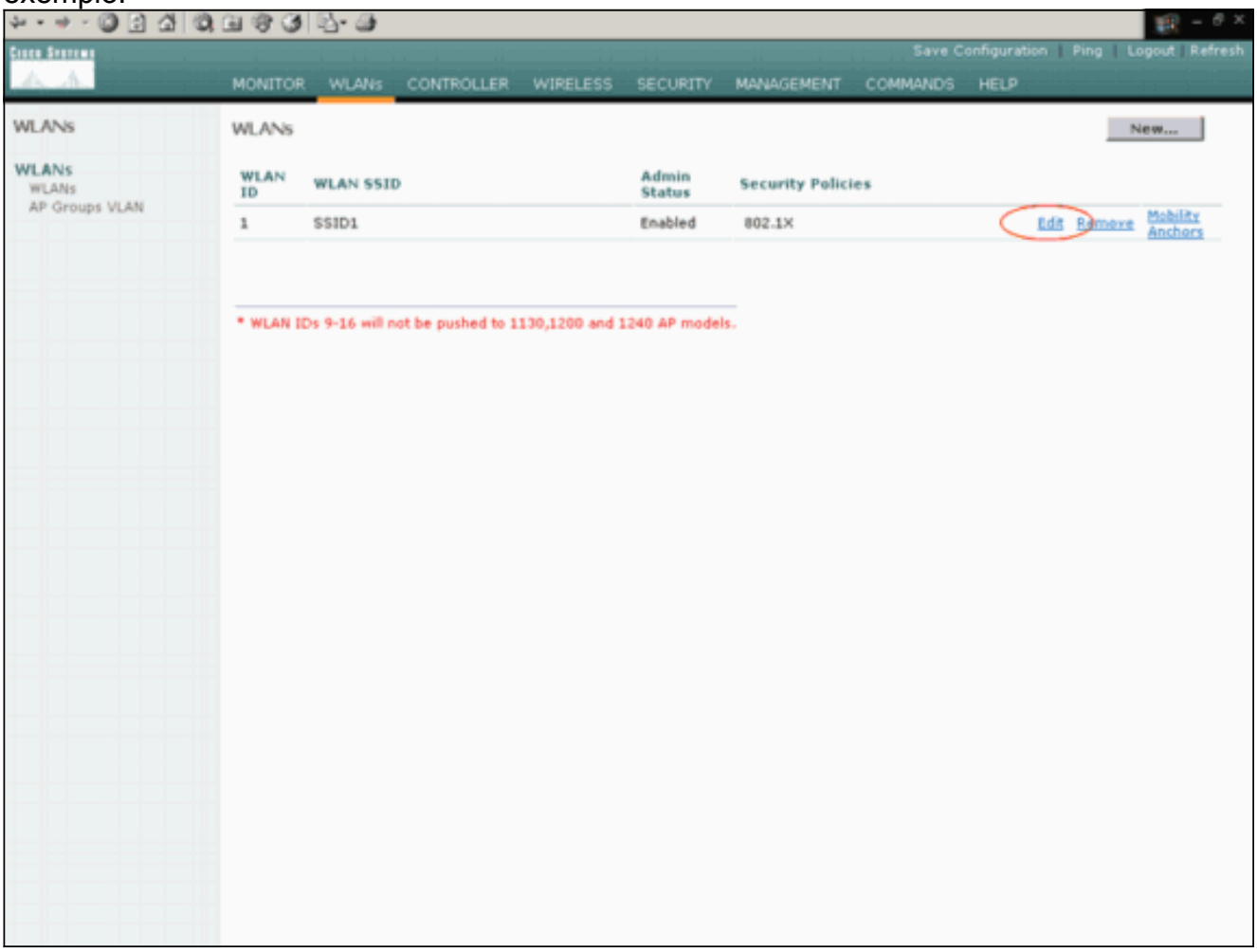
Este exemplo configura estes parâmetros na WLC:

- Nome do sistema
- Endereço IP da interface de gerenciamento
- Endereço IP da interface do gerenciador de AP
- Número da porta da interface de gerenciamento
- Identificador VLAN da interface de gerenciamento

- Nome do grupo de mobilidade
- SSID
- Muitos outros parâmetros

Esses parâmetros são usados para configurar a WLC para a operação básica. Como a saída da WLC nesta seção mostra, a WLC usa 172.16.1.50 como o endereço IP da interface de gerenciamento e 172.16.1.51 como o endereço IP da interface do gerenciador de AP. Para configurar as duas WLANs para sua rede, faça o seguinte na WLC:

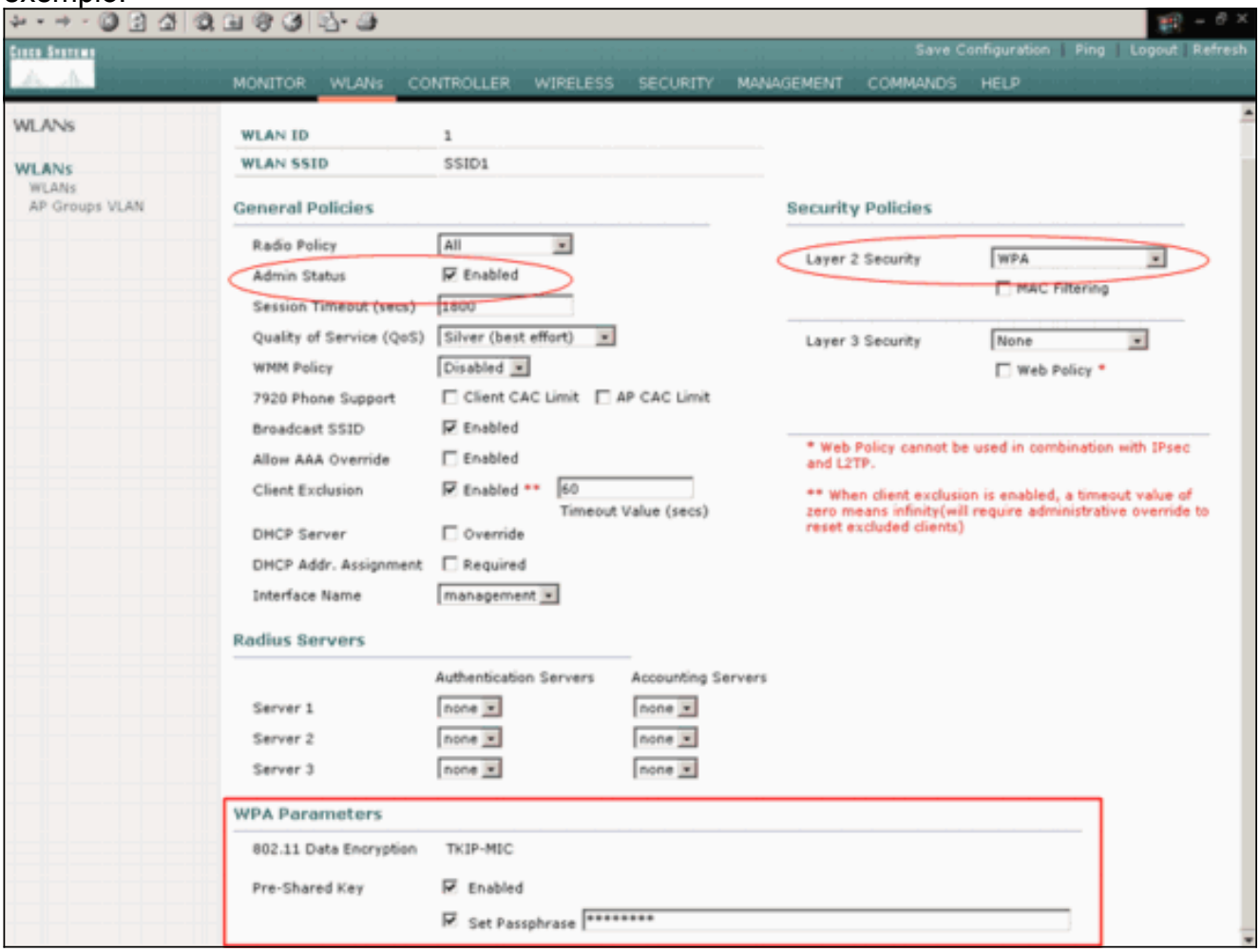
1. Na GUI da WLC, clique em **WLANs** no menu na parte superior da janela.A janela WLANs será exibida. Essa janela lista as WLANs configuradas na WLC. Como você configurou uma WLAN com o uso do assistente de configuração de inicialização, você deve configurar os outros parâmetros para esta WLAN.
2. Clique em **Edit** para o SSID1 da WLAN.Aqui está um exemplo:



A janela WLANs > Edit é exibida. Nessa janela, você pode configurar os parâmetros específicos da WLAN, que inclui Políticas gerais, Políticas de segurança, servidor RADIUS e outros.

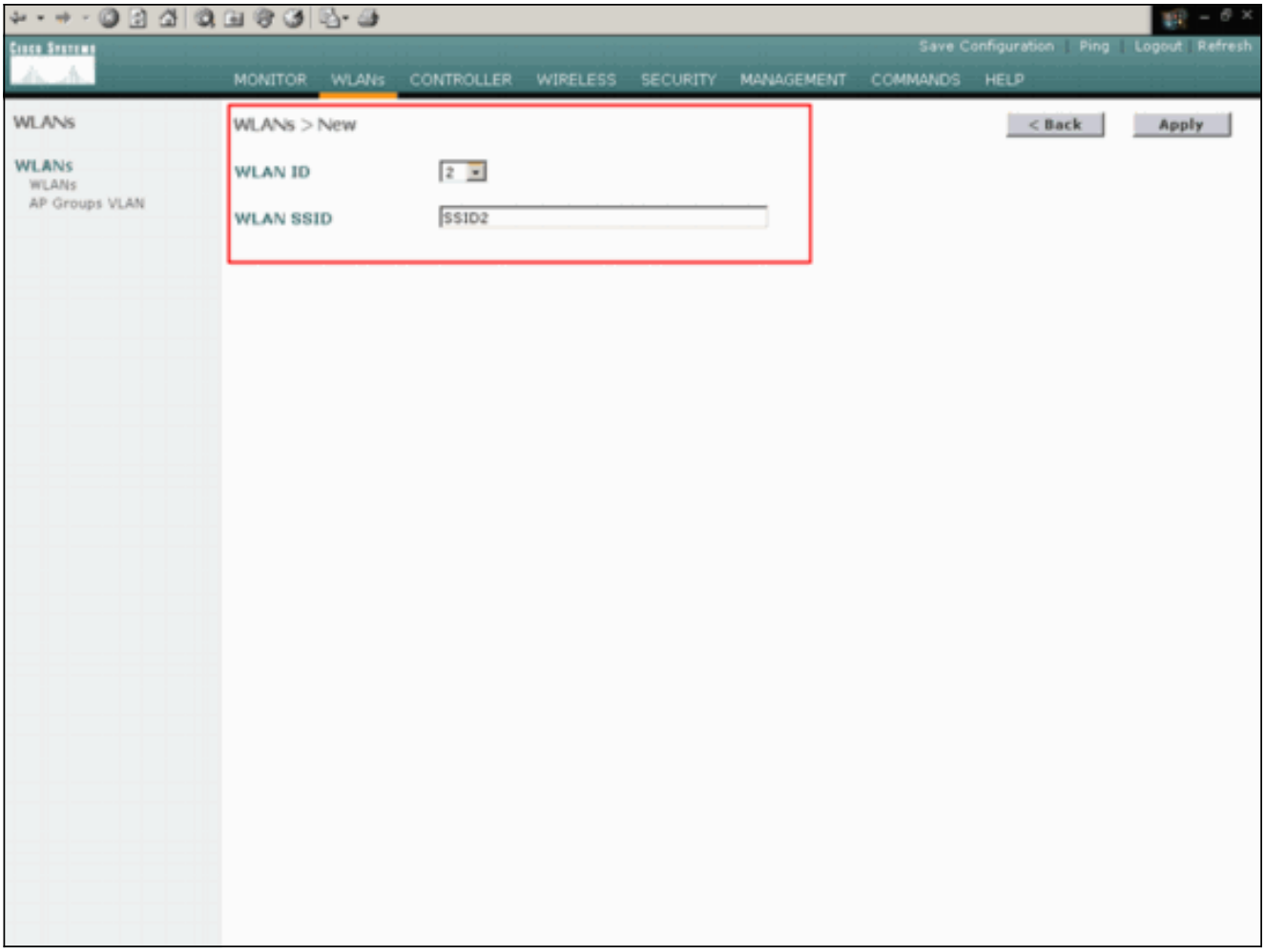
3. Faça estas seleções na janela WLANs > Editar:Na área de Políticas gerais, marque a caixa de seleção **Habilitado** ao lado de Status do administrador para habilitar essa WLAN.Escolha **WPA** no menu suspenso Layer 2 Security para usar WPA para WLAN 1.Defina os parâmetros WPA na parte inferior da janela.Para usar WPA-PSK na WLAN 1, marque a caixa de seleção **Habilitado** ao lado de Chave pré-compartilhada na área Parâmetros WPA e digite a senha para WPA-PSK. A WPA-PSK usará TKIP para criptografia.**Observação:** a senha WPA-PSK deve corresponder à senha configurada no adaptador cliente para que a WPA-PSK funcione.Clique em Apply.Aqui está um

exemplo:



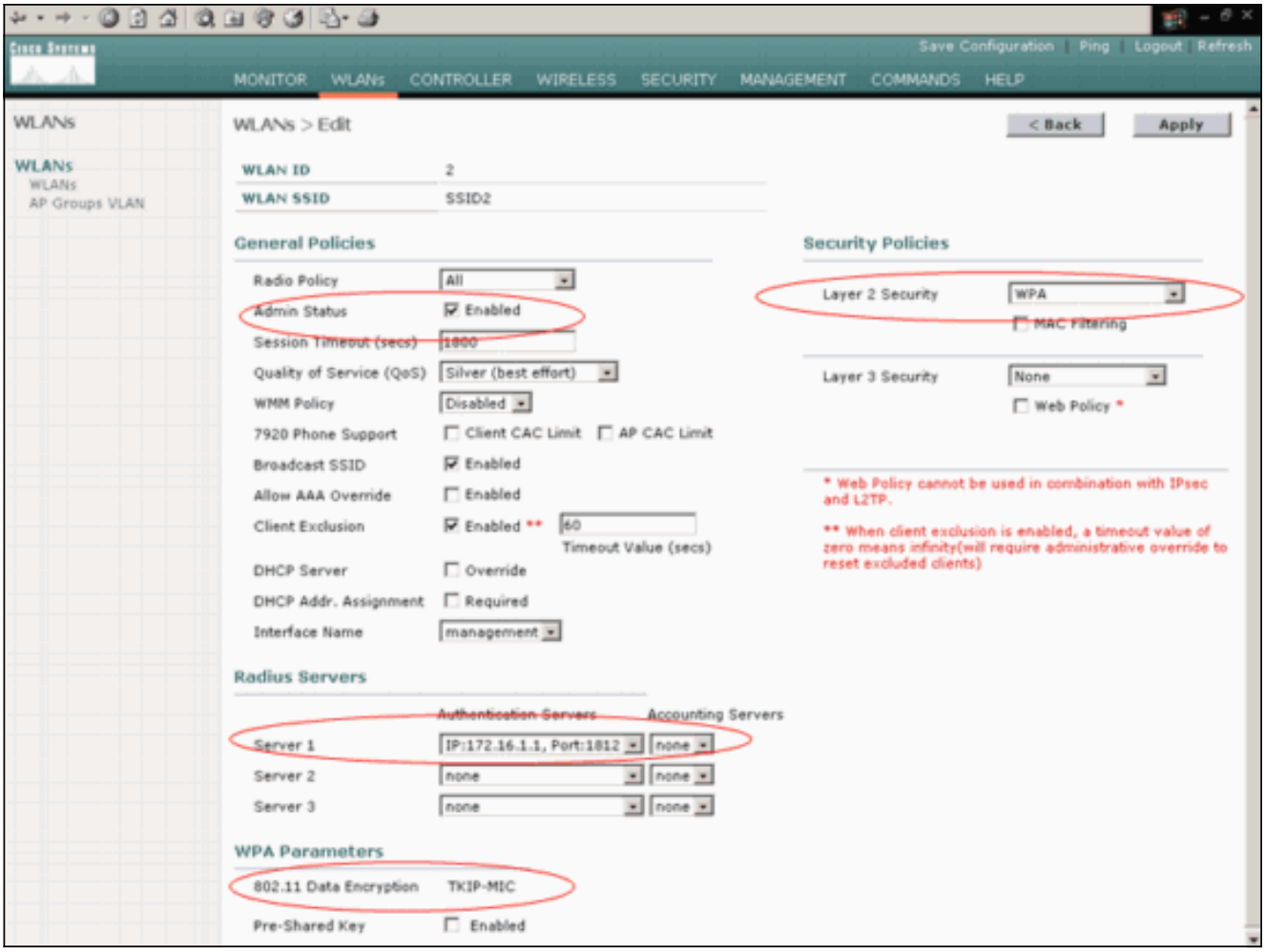
Você configurou a WLAN 1 para a criptografia WPA-PSK.

4. Para definir a WLAN 2, clique em **New** na janela WLANs.A janela WLAN > New é exibida.
5. Na janela WLAN > New, defina o ID da WLAN e o SSID da WLAN e clique em **Apply**.Aqui está um
   exemplo:



A janela WLAN > Edit para a segunda WLAN é exibida.

6. Faça estas seleções na janela WLANs > Editar:Na área de Políticas gerais, marque a caixa de seleção **Habilitado** ao lado de Status do administrador para habilitar essa WLAN.Escolha **WPA** no menu suspenso Layer 2 Security para configurar a WPA para esta WLAN.Na área Servidores Radius, escolha o servidor RADIUS apropriado a ser usado para autenticação dos clientes.Clique em Apply.Aqui está um
exemplo:



Observação: este documento não explica como configurar os servidores RADIUS e a autenticação EAP. Para obter informações sobre como configurar a autenticação EAP com WLCs, consulte o Exemplo de Configuração de Autenticação EAP com Controladores WLAN (WLC).

Prima o AP para instalação no local remoto

Primagem é um processo pelo qual os LAPs obtêm uma lista de controladores aos quais podem se conectar. Os LAPs são informados de todos os controladores no grupo de mobilidade assim que se conectam a um único controlador. Dessa forma, os LAPs aprendem todas as informações necessárias para se unirem a qualquer controlador no grupo.

Para preparar um AP com capacidade para REAP, conecte o AP à rede com fio no escritório principal. Essa conexão permite que o AP descubra um único controlador. Depois que o LAP ingressa no controlador no escritório central, o AP faz o download da versão do sistema operacional (SO) do AP que corresponde à infraestrutura da WLAN e à configuração. Os endereços IP de todas as controladoras no grupo de mobilidade são transferidos para o AP. Quando o AP tem todas as informações necessárias, ele pode ser conectado no local remoto. O AP pode então descobrir e se juntar ao controlador menos utilizado da lista, se a conectividade IP estiver disponível.

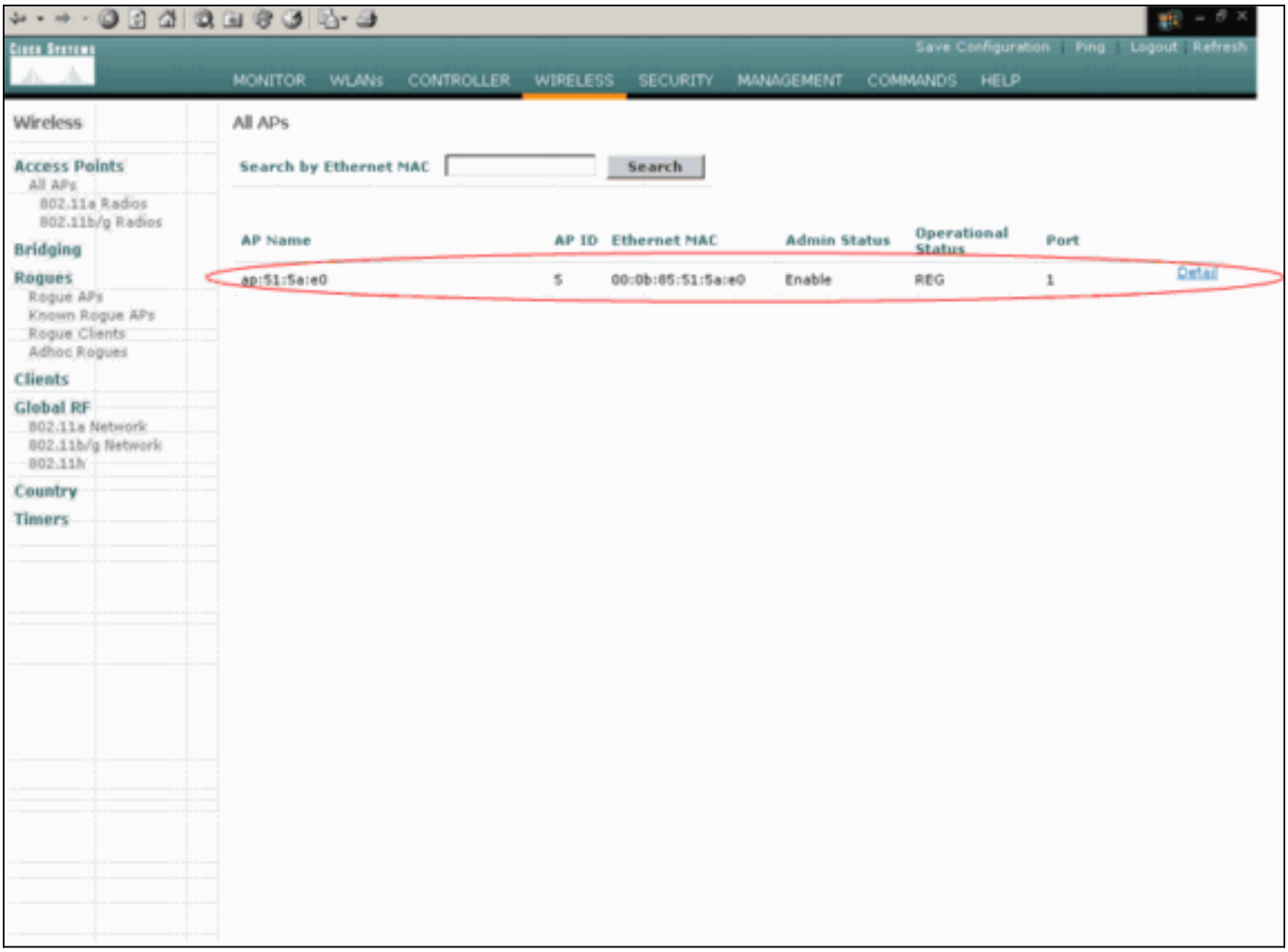
Observação: certifique-se de definir os APs para o modo "REAP" antes de desligá-los para enviá-los para os locais remotos. Você pode definir o modo no nível do AP através da CLI ou GUI do controlador ou com o uso de modelos do Wireless Control System (WCS). Os APs são definidos para executar a funcionalidade "local" regular por padrão.

Os LAPs podem usar qualquer um destes métodos para descobrir a controladora:

- **Descoberta da camada 2**
- **Descoberta da camada 3**Com o uso de um broadcast de sub-rede localCom o uso da opção de DHCP 43Com o uso de um servidor DNSCom o uso de OTAP (Over-the-Air Provisioning, provisionamento por excesso de ar)Com o uso de um servidor DHCP interno**Observação:** para usar um servidor DHCP interno, o LAP deve se conectar diretamente à WLC.

Este documento pressupõe que o LAP se registra na WLC com o uso do mecanismo de descoberta da opção 43 do DHCP. Para obter mais informações sobre o uso da opção de DHCP 43 para registrar o LAP na controladora, assim como outros mecanismos de descoberta, consulte Registro de AP Lightweight (LAP) em uma Controladora de LAN Wireless (WLC).

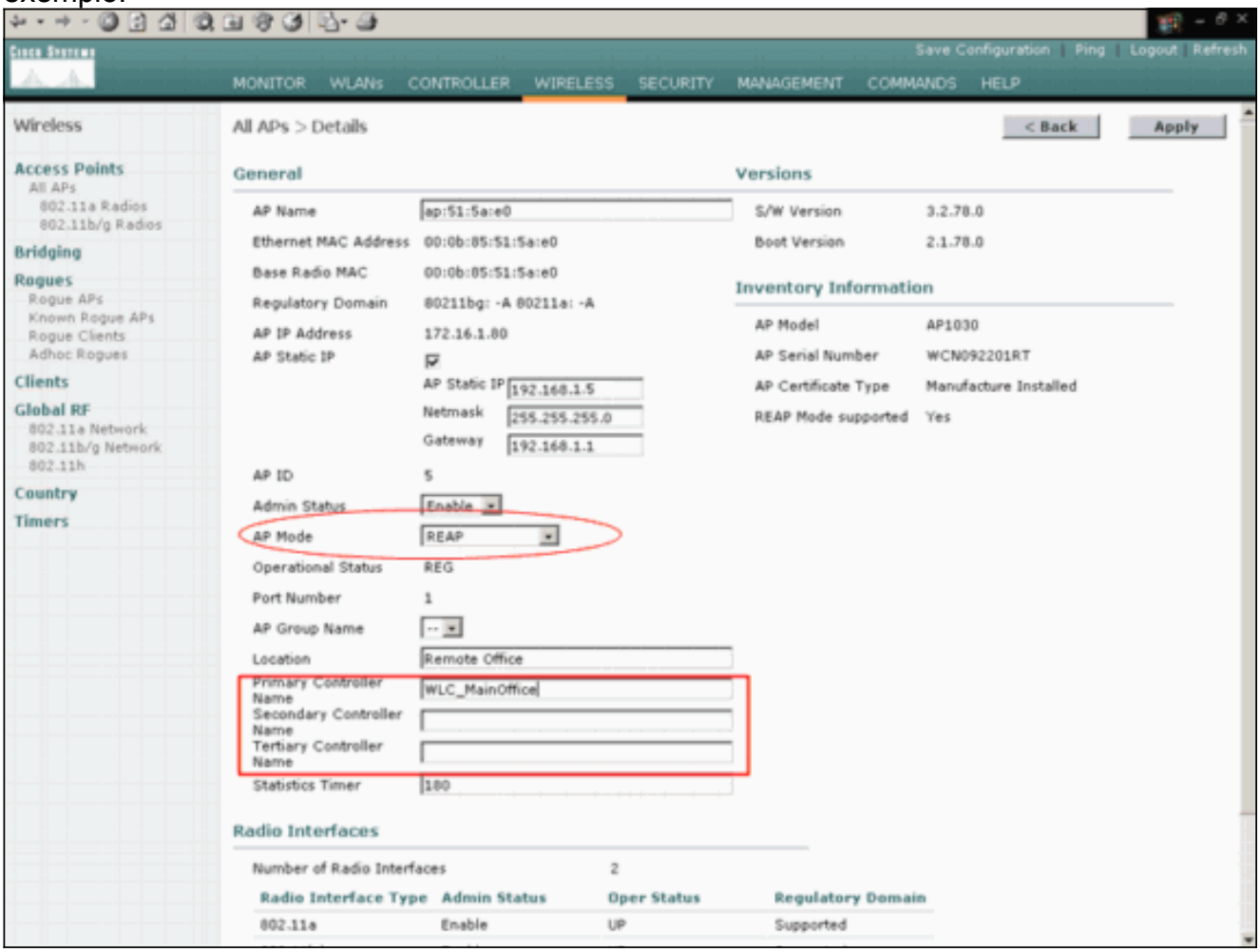
Depois que o LAP descobrir a controladora, você poderá ver que o AP está registrado na controladora na janela Wireless da WLC. Aqui está um exemplo:



Conclua estes passos para configurar o LAP para o modo REAP normal:

1. Na GUI do WLC, clique em **Wireless**.A janela Todos os APs é exibida. Essa janela lista os APs registrados na WLC.
2. Selecione o AP que você deve configurar para o modo REAP e clique em **Detalhes**.A janela Todos os APs > Detalhes do AP específico é exibida. Nesta janela, você pode configurar os vários parâmetros do AP, que incluem:nome de APEndereço IP (que pode ser alterado para estático)Status do administradorParâmetros de segurançamodo APLista de WLCs às quais o AP pode se conectarOutros parâmetros
3. Escolha **REAP** no menu suspenso AP Mode (Modo AP).Esse modo só está disponível em APs compatíveis com REAP.

4. Defina os nomes do controlador que os APs usarão para registrar e clique em **Aplicar**.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.Aqui está um exemplo:



Você configurou o AP para o modo REAP e pode implantá-lo no local remoto.

Observação: nesta janela de exemplo, você pode ver que o endereço IP do AP é alterado para estático e um endereço IP estático 192.168.1.5 é atribuído. Esta atribuição ocorre porque esta é a sub-rede a ser usada no escritório remoto. Assim, você usa o endereço IP do servidor DHCP, 172.16.1.80, somente durante o estágio de preparação. Depois que o AP for registrado no controlador, você alterará o endereço para um endereço IP estático.

Configurar os 2800 Routers para estabelecer o link da WAN

Para estabelecer o link da WAN, este exemplo usa dois roteadores da série 2800 com OSPF para rotear informações entre as redes. Aqui está a configuração de ambos os roteadores para o exemplo de cenário neste documento:

Escritório principal

`MainOffice#show run`
`Building configuration...`
 	
`Current configuration : 728 bytes`

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname MainOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 172.16.1.60 255.255.0.0
!--- This is the interface which acts as the default
gateway to the WLC. ! interface Virtual-Template1 no ip
address ! interface Serial0 no ip address ! interface
Serial1 !--- This is the interface for the WAN link. ip
address 10.0.0.1 255.0.0.0 encapsulation ppp !--- This
example uses PPP. Use the appropriate !--- encapsulation
for the WAN connection. ! router ospf 50 !--- Use OSPF
to route data between the different networks. log-
adjacency-changes network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.0.255.255 area 0 ! ! ip classless
ip http server ! ! ! line con 0 line aux 0 line vty 0 4
! end
```

Filial

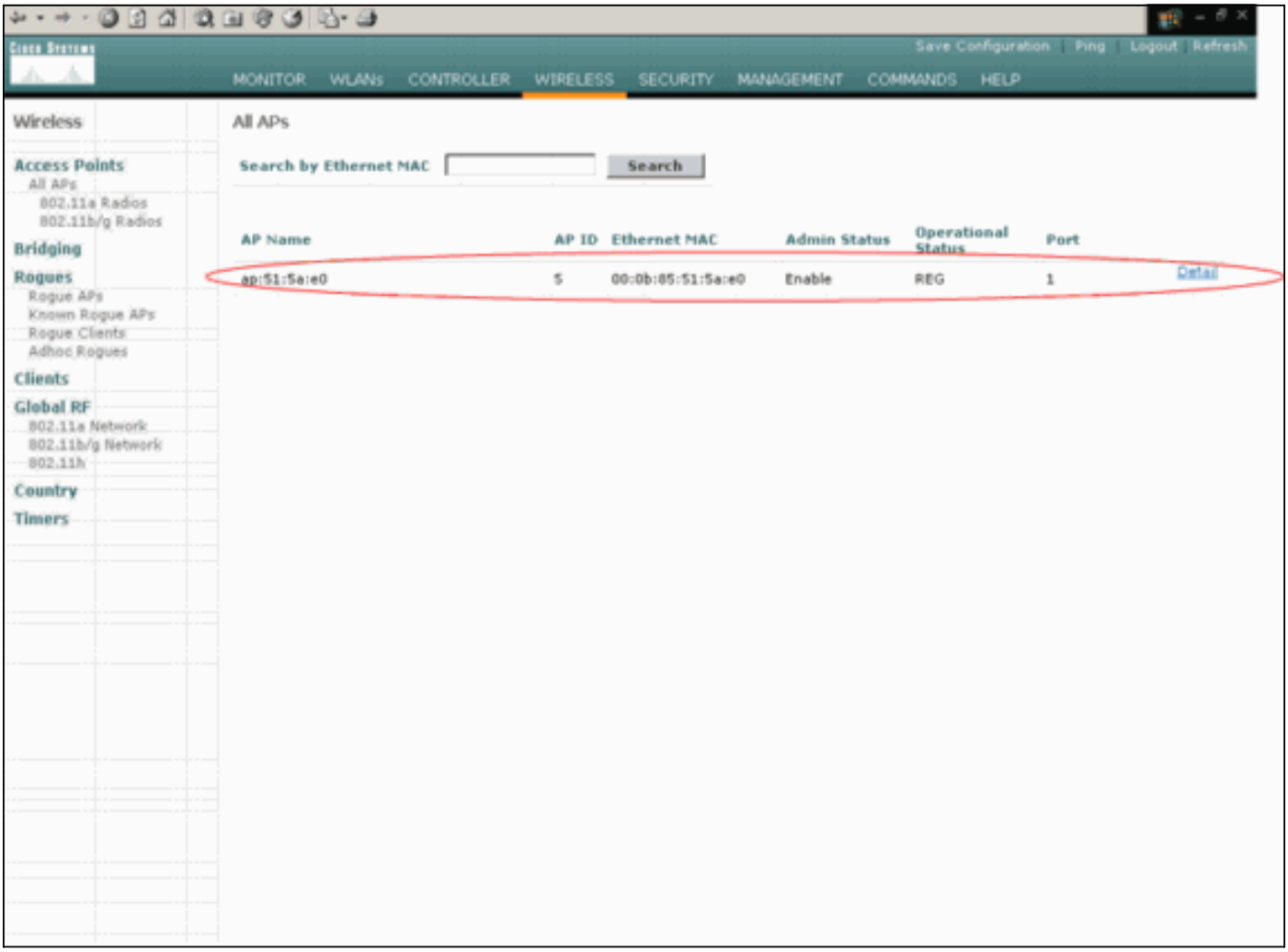
```
BranchOffice#show run
Building configuration...

Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!--- This is the interface which acts as the default
gateway to the LAP. ! interface Serial0 no ip address !
interface Serial1 !--- This is the interface for the WAN
link. ip address 10.0.0.2 255.0.0.0 encapsulation ppp
clockrate 56000 ! router ospf 50 !--- Use OSPF to route
data between the different networks. log-adjacency-
changes network 10.0.0.0 0.255.255.255 area 0 network
192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
autocommand access enable-timeout 2 ! end
```

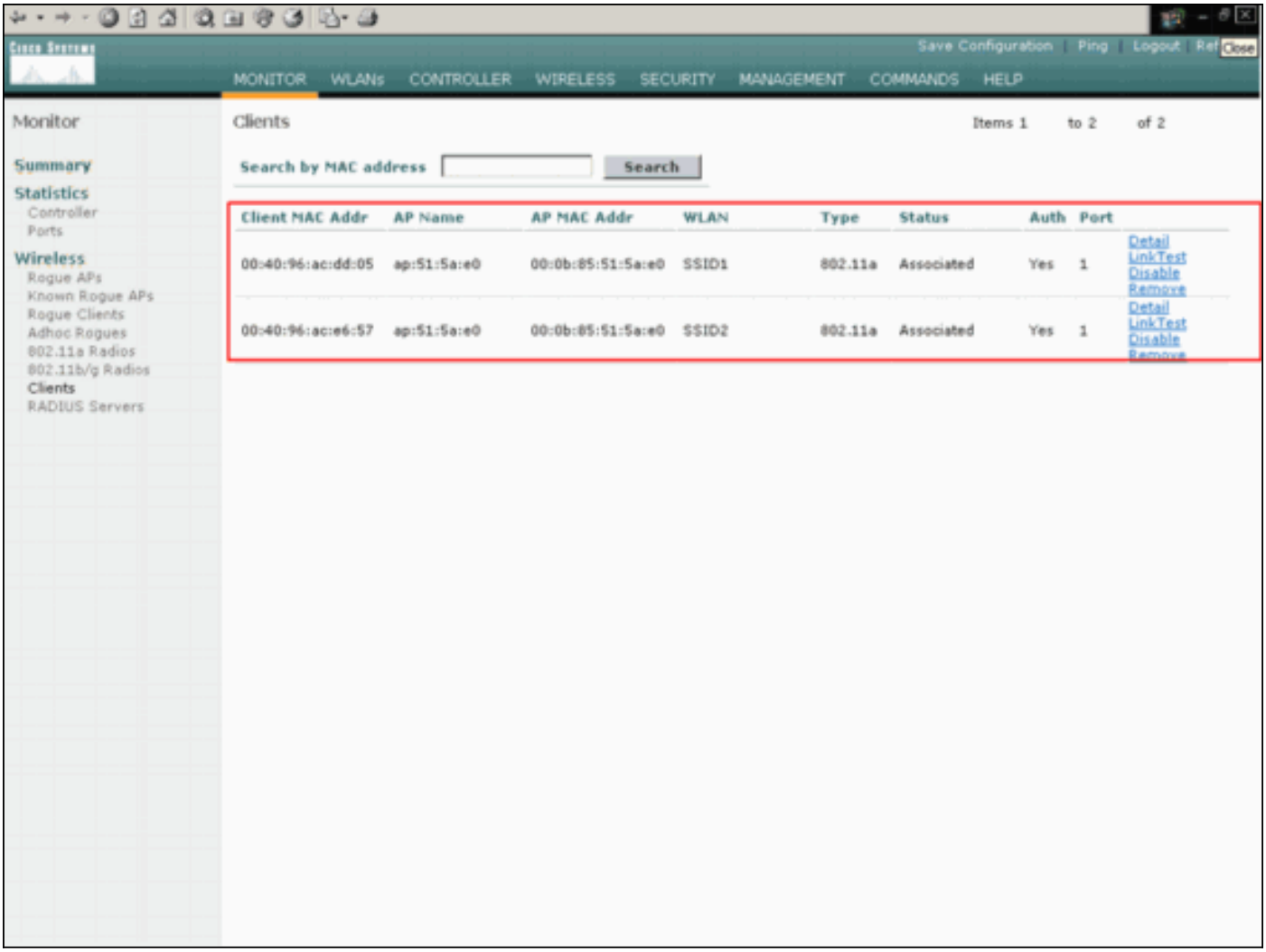
Implantar o AP do REAP no local remoto

Agora que você configurou as WLANs nas WLCs, primou o LAP e estabeleceu o link da WAN entre o escritório central e o escritório remoto, você está pronto para implantar o AP no local remoto.

Depois de ligar o AP no local remoto, o AP procura o controlador na ordem em que você configurou no estágio de preparação. Depois que o AP localiza o controlador, o AP se registra com o controlador. Exemplo: Na WLC, você pode ver que o AP se uniu à controladora na porta 1:



Clientes que têm o SSID **SSID1** e para os quais o WPA-PSK está ativado, associem-se ao AP na WLAN 1. Clientes que têm o SSID **SSID2** e que têm a autenticação 802.1x ativada, associem-se ao AP na WLAN 2. Aqui está um exemplo que mostra dois clientes. Um cliente está conectado à WLAN 1 e o outro está conectado à WLAN 2:



Verificar

Use esta seção para confirmar se a configuração do REAP está funcionando corretamente.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Desative o link da WAN. Quando o link da WAN está inoperante, o AP perde a conectividade com a WLC. Em seguida, a WLC cancela o registro do AP de sua lista. Aqui está um exemplo:

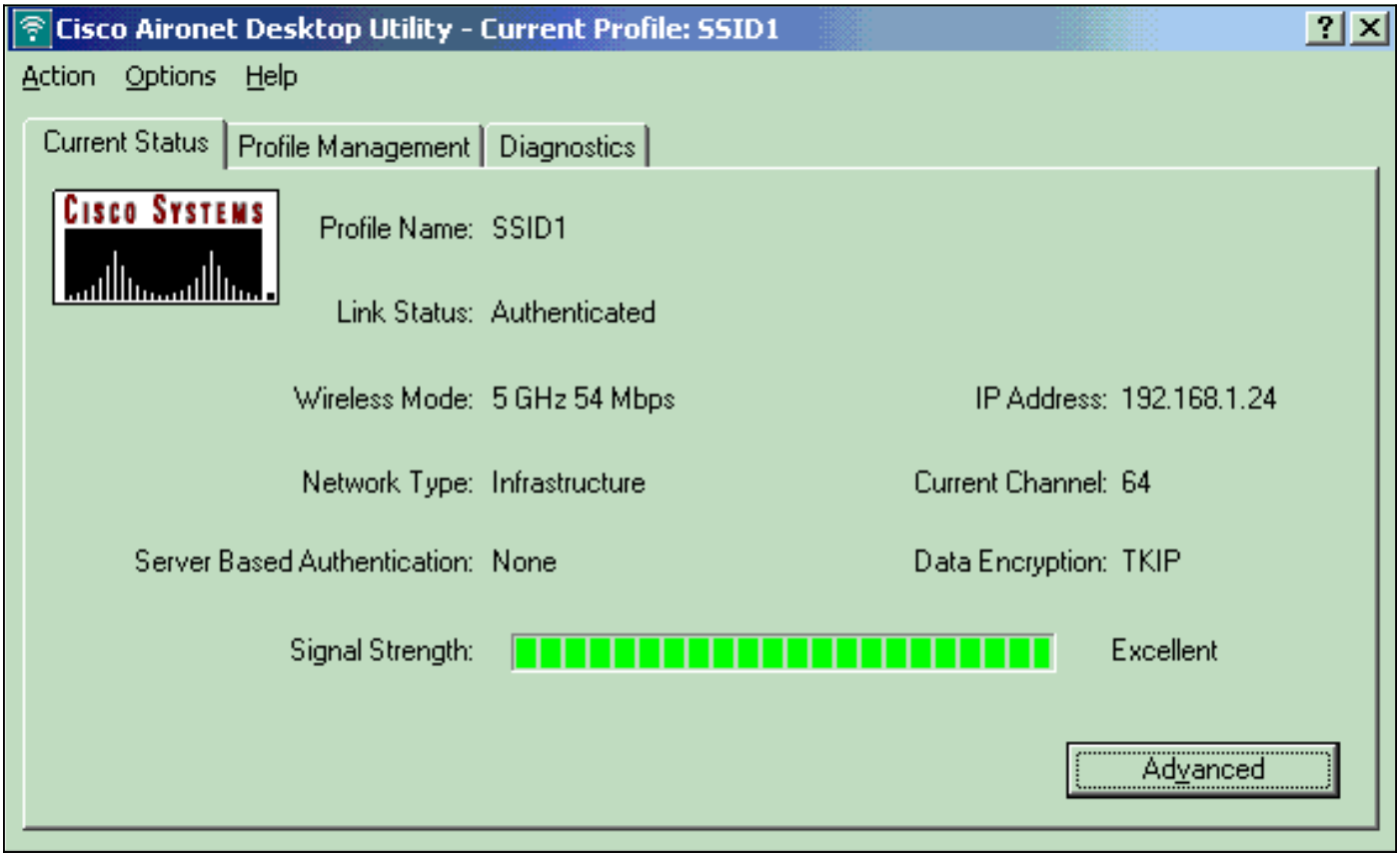
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP
00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
```

```
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

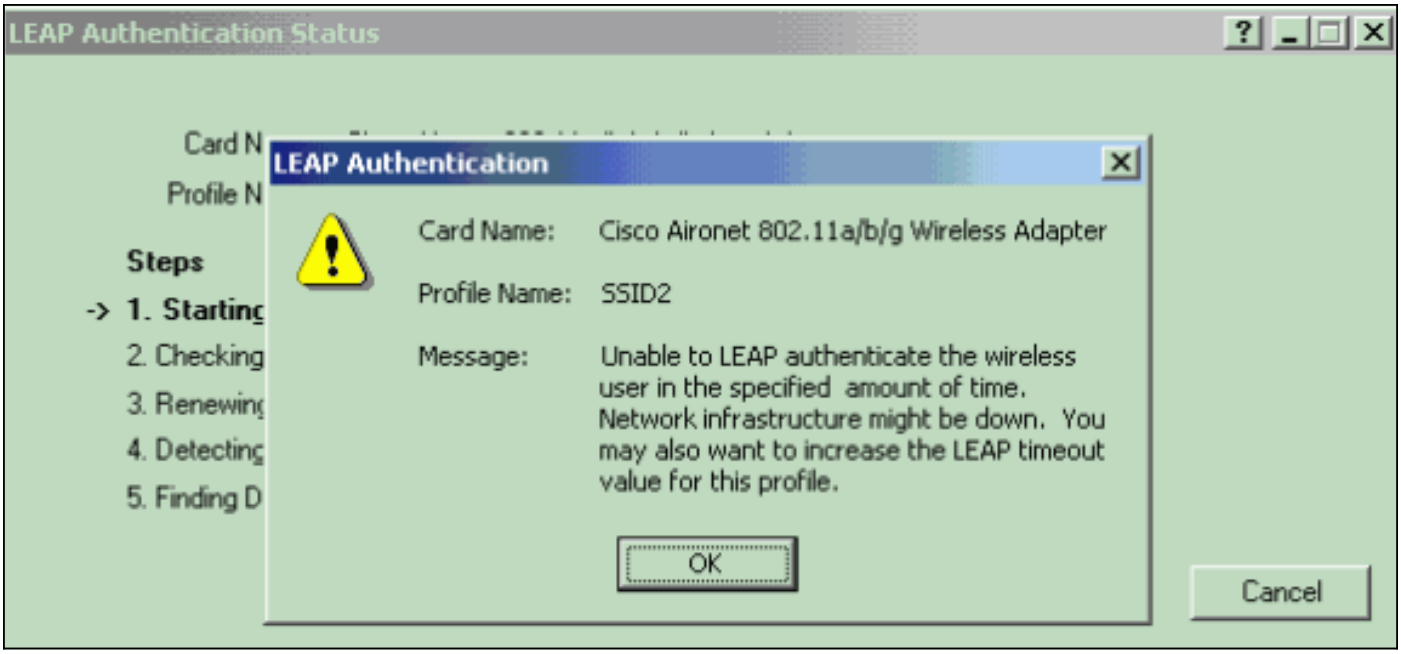
Na saída do comando **debug lwapp events enable**, você pode ver que a WLC anula o registro do AP porque a WLC não recebeu uma resposta de pulsação do AP. Uma resposta de pulsação é semelhante a mensagens de keepalive. O controlador tenta cinco batimentos de coração consecutivos, separados por um segundo. Se a WLC não receber uma resposta, a WLC cancelará o registro do AP.

Quando o AP está no modo autônomo, o LED de energia do AP pisca. Os clientes que se associam à primeira WLAN (WLAN 1) ainda estão associados ao AP porque os clientes na primeira WLAN estão configurados somente para a criptografia WPA-PSK. O LAP lida com a própria criptografia no modo autônomo. Este é um exemplo que mostra o status (quando o link da WAN está inativo) de um cliente conectado à WLAN 1 com SSID1 e WPA-PSK:

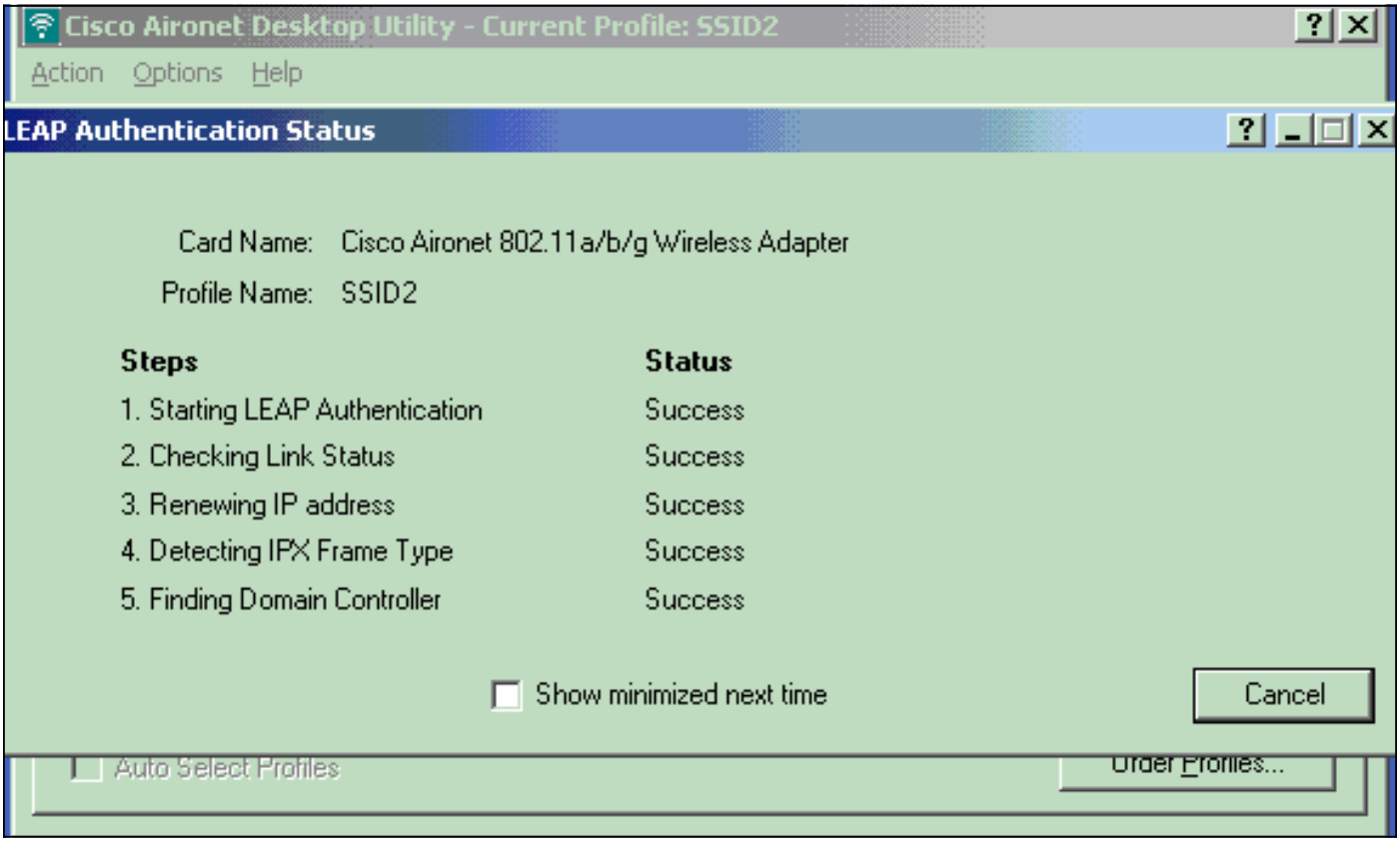
Observação: TKIP é a criptografia usada com WPA-PSK.



Os clientes conectados à WLAN 2 são desconectados porque a WLAN 2 usa autenticação EAP. Essa desconexão ocorre porque os clientes que usam autenticação EAP precisam se comunicar com a WLC. Esta é uma janela de exemplo que mostra que a autenticação EAP falha quando o link WAN está inativo:



Depois que o link da WAN estiver ativo, o AP volta ao modo REAP normal e se registra com o controlador. O cliente que usa a autenticação EAP também é ativado. Aqui está um exemplo:



Este exemplo de saída do comando **debug lwapp events enable** no controlador mostra estes resultados:

```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:06:40 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:51:5a:e0 on Port 1
Wed May 17 15:06:52 2006: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to
00:0b:85:33:84:a0 on port '1'
Wed May 17 15:06:52 2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500,
remote debug mode is 0
```

```
Wed May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51)
Switch IP: 172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP
Port: 5550, next hop MAC: 00:d0:58:ad:ae:cb
Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply to AP
00:0b:85:51:5a:e0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1,
192.168.1.5/255.255.255.0, gtw 192.168.1.1
```

Troubleshoot

Use esta seção para resolver problemas de configuração.

Comandos para Troubleshooting

Você pode usar esses comandos **debug** para solucionar problemas da configuração.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug lwapp events enable** — Exibe a sequência de eventos que ocorrem entre o LAP e a WLC.
- **debug lwapp errors enable** — Exibe os erros que ocorrem na comunicação LWAPP.
- **debug lwapp packet enable** —Exibe a depuração de um rastreamento de pacote LWAPP.
- **debug mac addr** —Ativa a depuração de MAC para o cliente que você especificar.

Informações Relacionadas

- Guia de implantação do REAP na filial
- Exemplo de Configuração de Autenticação EAP com Controladores WLAN (WLC)
- Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight
- Exemplo de Configuração de Failover do Controlador WLAN para Pontos de Acesso Lightweight
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems