

Remoto-borda AP (COLHA) com AP de pouco peso e exemplo de configuração dos controladores do Wireless LAN (WLC)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o WLC para a operação básica e configurar WLAN](#)

[Apronte o AP para a instalação no local remoto](#)

[Configurar os 2800 Router para estabelecer o link MACILENTO](#)

[Distribua a COLHEITA AP no local remoto](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

As capacidades do Access point da Remoto-borda (COLHA) introduzidas com rede de Cisco Unified Wireless permitem o desenvolvimento remoto dos Access point da leve Cisco (regaços) do controlador do Wireless LAN (WLAN) (WLC). Isto faz-lhes o ideal para o escritório filial e lugar varejos pequenos. Este documento explica como implementa uma rede WLAN com base em REAP com uso do Cisco 1030 Series LAP e do 4400 WLCs.

Pré-requisitos

Requisitos

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

- Conhecimento dos WLC e como configurar os parâmetros básicos WLC
- Conhecimento do modo da COLHEITA de operação em Cisco 1030 REGAÇOS
- Conhecimento da configuração de um servidor de DHCP externo e/ou de um server do

Domain Name System (DNS)

- Conhecimento de conceitos do Wi-Fi Protected Access (WPA)

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa a versão de firmware 4.2
- Cisco 1030 REGAÇOS
- Dois Cisco 2800 Series Router que executam o Software Release 12.2(13)T13 de Cisco IOS®
- Adaptador cliente do Cisco Aironet 802.11a/b/g que executa o 3.0 da versão de firmware
- 3.0 da versão de utilitário de desktop do Cisco Aironet

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

COLHA o modo permite um REGAÇO de residir através de um link MACILENTO, e ainda possa comunicar-se com o WLC e fornecer a funcionalidade de um REGAÇO regular. COLHA o modo é apoiado somente nos 1030 regaços neste momento.

A fim fornecer esta funcionalidade, os 1030 COLHEM separam o plano de pouco peso do controle do protocolo do Access point (LWAPP) do plano wireless dos dados. Cisco WLC é usado ainda para o controle centralizado e o Gerenciamento da mesma forma que os Access point LWAPP-baseados regulares (AP) estão usados, quando todos os dados do usuário forem construídos uma ponte sobre localmente no AP. O acesso aos recursos de rede local é mantido durante todo interrupções de WAN.

COLHA o modo do apoio dois AP de operação:

- Modo normal REAP
- Modo independente

O REGAÇO está ajustado no modo normal REAP quando o link MACILENTO entre a COLHEITA AP e o WLC está acima. Quando os regaços se operam no modo normal REAP, podem apoiar até 16 WLAN.

Quando o link MACILENTO entre o WLC e o REGAÇO vai para baixo, o REGAÇO Colher-permitido comuta ao modo independente. Quando no modo independente, os regaços da COLHEITA puderem apoiar somente um WLAN independentemente sem o WLC, se o WLAN é configurado com o Wired Equivalent Privacy (WEP) ou o qualquer método de autenticação local. Neste caso, o WLAN que a COLHEITA AP apoia é o primeiro WLAN que é configurado no AP,

WLAN 1. Isto é porque a maioria dos outros métodos de autenticação precisam de passar a informação a e do controlador e, quando o link MACILENTO está para baixo, desta operação não são possíveis. No modo independente, os regaços apoiam um conjunto mínimo de características. Esta tabela mostra o conjunto de recurso que um REGAÇO da COLHEITA apoia quando reage do modo independente em comparação com as características que um REGAÇO da COLHEITA apoia no modo normal (quando o link MACILENTO é ascendente e uma comunicação ao WLC está acima):

Características que um REGAÇO da COLHEITA apoia no modo normal REAP e no modo independente

		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 os vlan múltiplos não estão apoiados em regaços REAP nos ambos os

modos. Os vlan múltiplos não são apoiados porque COLHA regaços pode somente residir em uma sub-rede única porque não podem executar a colocação de etiquetas do IEEE 802.1Q VLAN. Consequentemente, o tráfego em cada um dos service set identifier (SSID) termina na mesma sub-rede como a rede ligada com fio. Em consequência, o tráfego de dados não é separado na face da tela mesmo que o tráfego Wireless possa ser segmentado sobre o ar entre SSID.

Consulte [PARA COLHER o guia de distribuição no escritório filial](#) para obter mais informações sobre de COLHEM o desenvolvimento, e como controlar COLHA e suas limitações.

Configurar

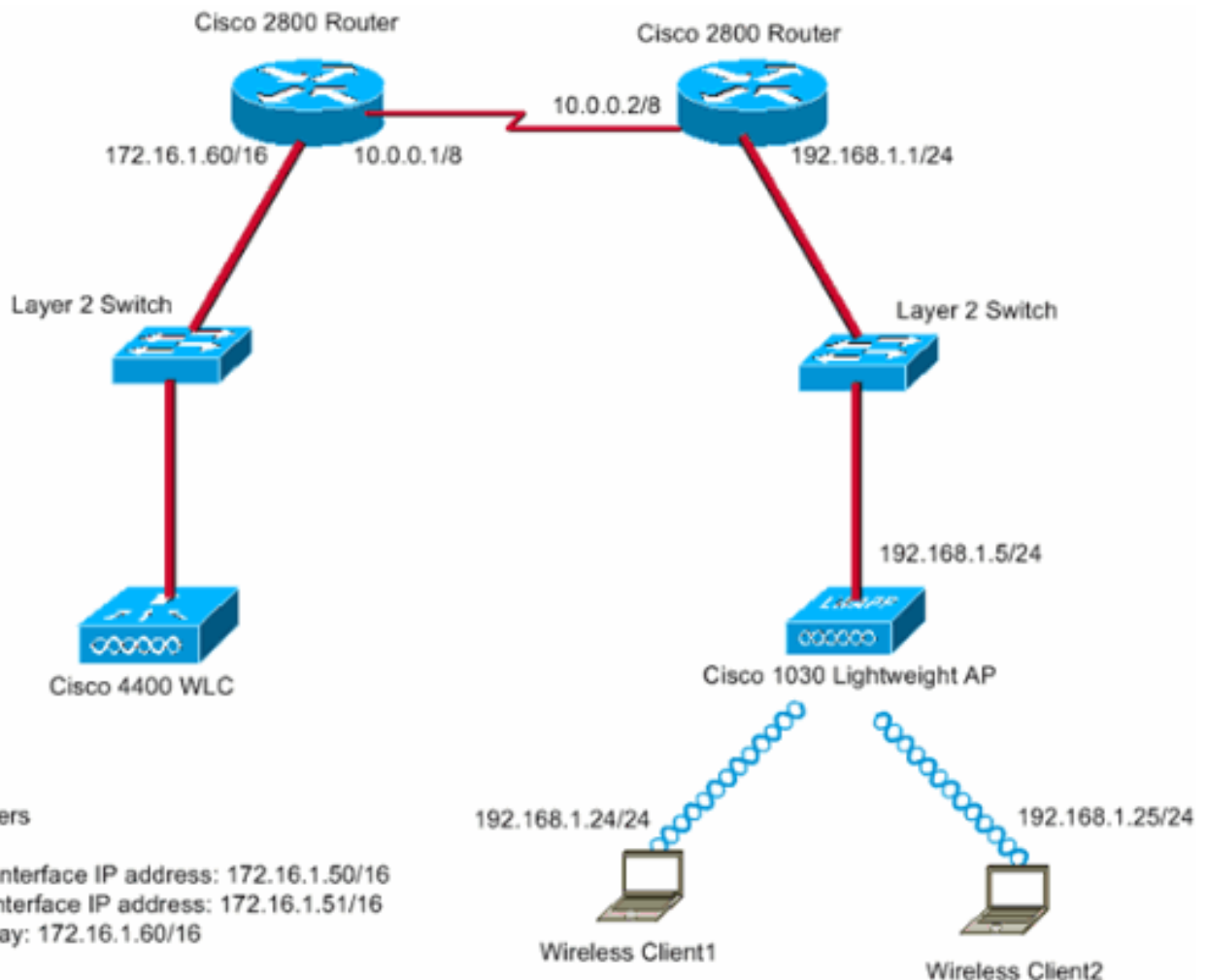
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

A fim configurar os dispositivos para executar a instalação de rede, termine estas etapas:

1. [Configurar o WLC para a operação básica e configurar WLAN.](#)
2. [Apronte o AP para a instalação no local remoto.](#)
3. [Configurar os 2800 Router para estabelecer o link MACILENTO.](#)
4. [Distribua o REGAÇO da COLHEITA no local remoto.](#)

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



O escritório principal conecta ao escritório filial com o uso de uma linha alugada. A linha alugada termina em 2800 Series Router em cada extremidade. Este exemplo usa o protocolo do Open Shortest Path First (OSPF) para distribuir dados no link MACILENTO com o encapsulamento PPP. Os 4400 WLC estão no escritório principal e os 1030 REGAÇOS devem ser distribuídos no escritório remoto. Os 1030 REGAÇOS devem apoiar dois WLAN. Estão aqui os parâmetros para os WLAN:

- **WLAN 1**SSID — **SSID1**Autenticação — **Abra**Criptografia — **Temporal Key Integrity Protocol (TKIP)** ([**WPA-PSK**] da **chave pré-compartilhada WPA**)
- **WLAN 2**SSID — **SSID2**Autenticação — **Extensible Authentication Protocol (EAP)**Criptografia — **TKIP****Nota:** Para WLAN 2, a configuração neste original usa o WPA (autenticação do 802.1x e TKIP para a criptografia).

Você deve configurar os dispositivos para esta instalação.

[Configurar o WLC para a operação básica e configurar WLAN](#)

Você pode usar o assistente da configuração de inicialização no comando line interface(cli) a fim configurar o WLC para a operação básica. Alternativamente, você pode igualmente usar o GUI a fim configurar o WLC. Este original explica a configuração no WLC com uso do assistente da configuração de inicialização no CLI.

Após as botas WLC pela primeira vez, participa diretamente no assistente da configuração de inicialização. Você usa o wizard de configuração para configurar configurações básicas. Você pode executar o assistente no CLI ou no GUI. Está aqui um exemplo do assistente da 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...

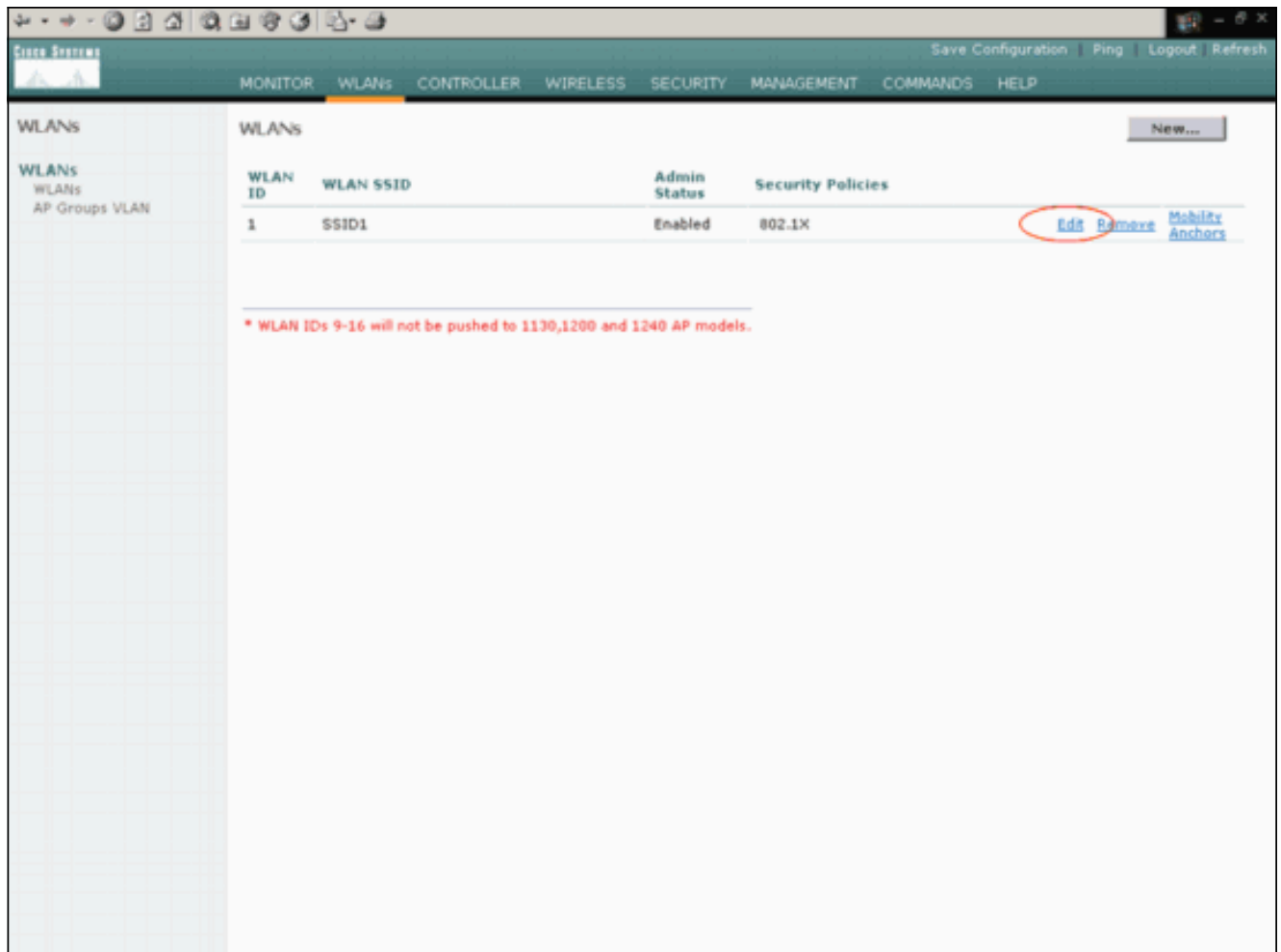
```

Este exemplo configura estes parâmetros no WLC:

- Nome de sistema
- Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento
- Endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do gerenciador AP
- Número de porta da interface de gerenciamento
- Identificador de VLAN da interface de gerenciamento
- Nome do grupo da mobilidade
- SSID
- Muitos outros parâmetros

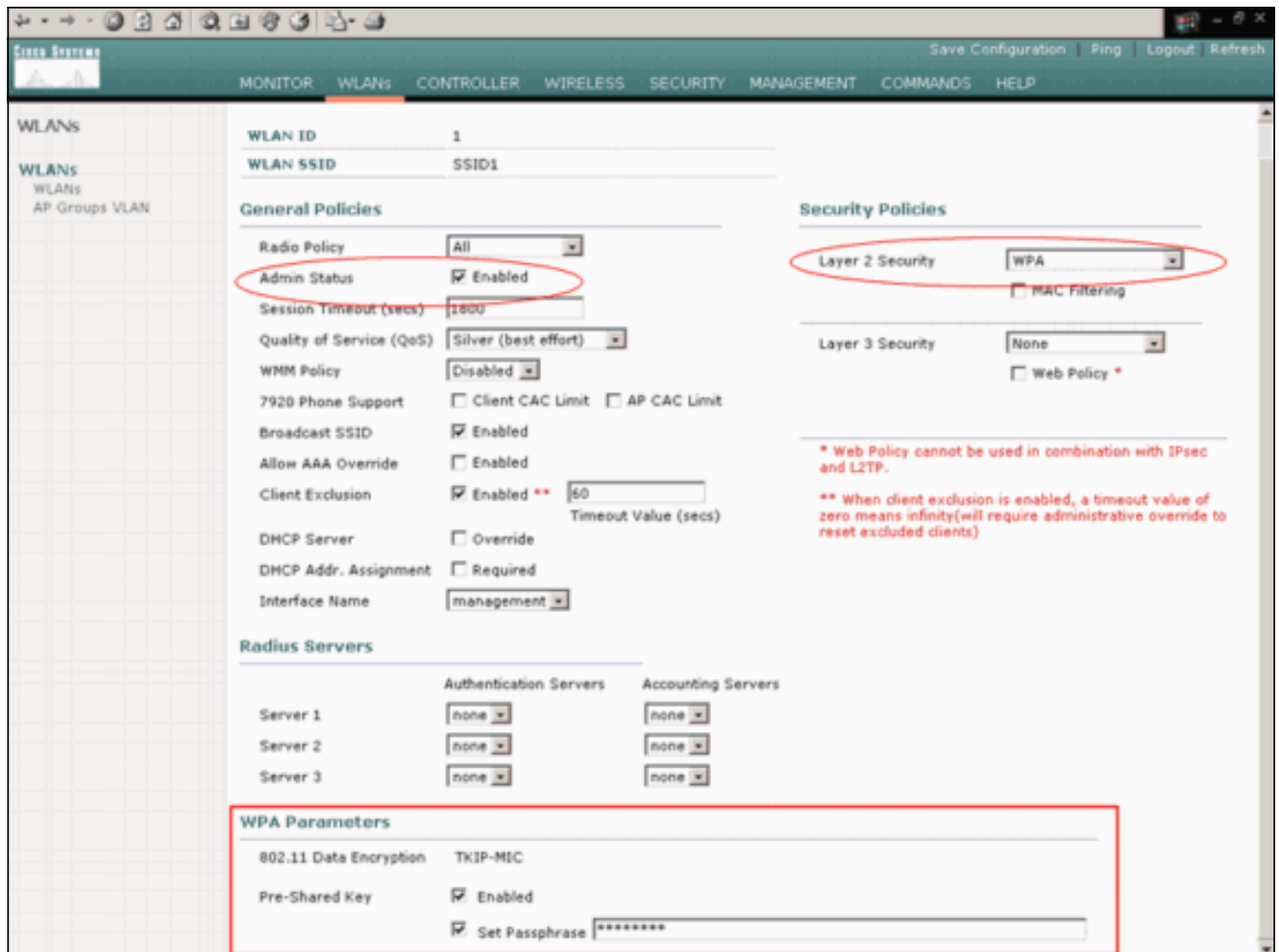
Estes parâmetros são usados para estabelecer o WLC para a operação básica. Enquanto a saída WLC nesta seção mostra, o WLC usa 172.16.1.50 como o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento e 172.16.1.51 como o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do gerenciador AP. A fim configurar os dois WLAN para sua rede, termine estas etapas no WLC:

1. Do WLC GUI, clique **WLAN no** menu na parte superior do indicador. A janela WLANs aparece. Este indicador alista os WLAN que são configurados no WLC. Porque você configurou um WLAN com uso do assistente da configuração de inicialização, você deve configurar os outros parâmetros para este WLAN.
2. O clique **edita** para o WLAN SSID1. Aqui está um exemplo:



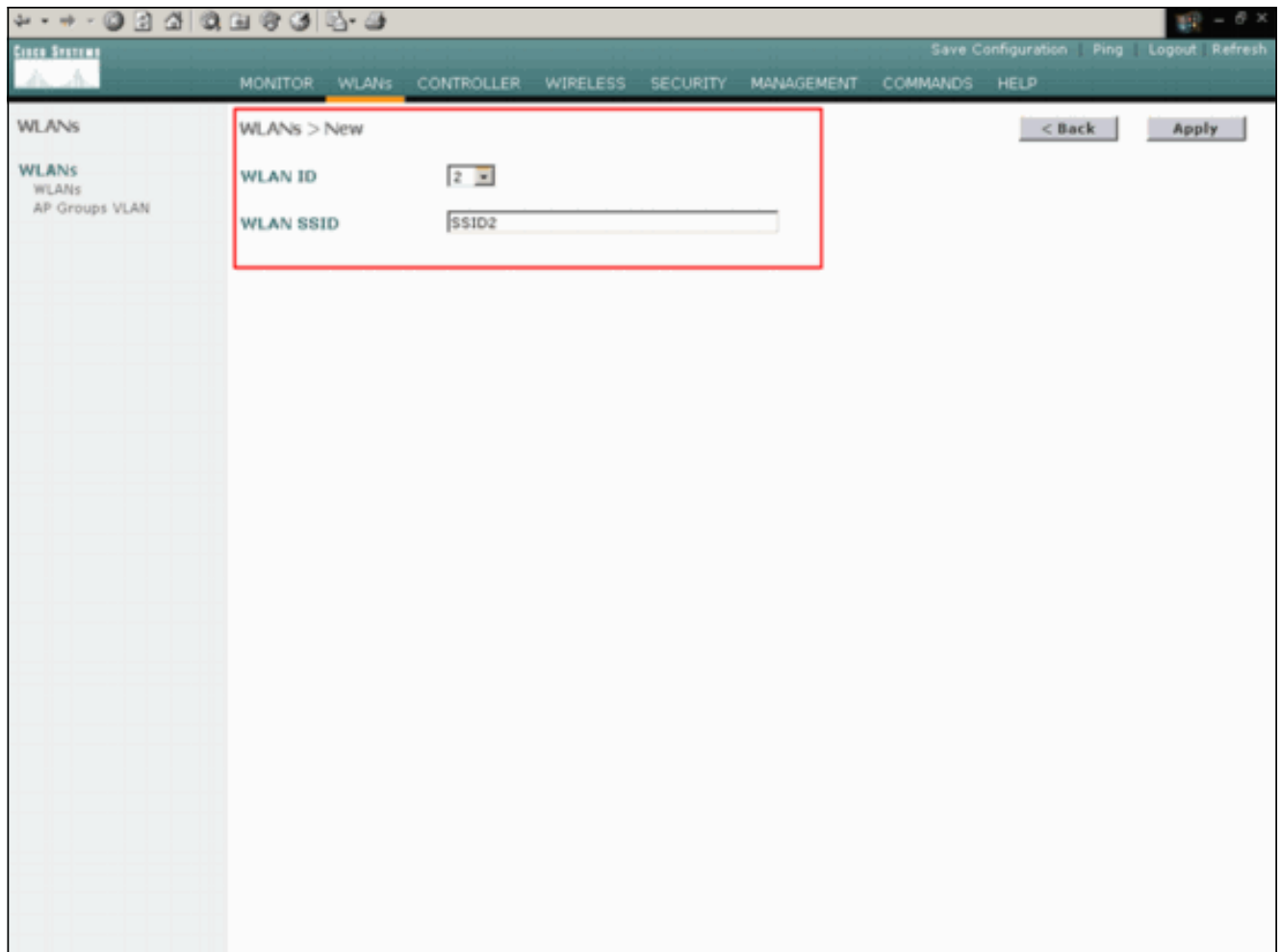
Os WLAN > editam o indicador aparecem. Neste indicador, você pode configurar os parâmetros que são específicos ao WLAN, que inclui políticas gerais, políticas de segurança, servidor Radius, e outro.

3. Faça estas seleções no WLAN > para editar o indicador: Na área de políticas gerais, verifique a caixa de verificação **permitida** ao lado do status administrativo a fim permitir este WLAN. Escolha o **WPA do** menu suspenso da Segurança da camada 2 a fim usar o WPA para WLAN 1. Defina os parâmetros WPA na parte inferior do indicador. A fim usar o WPA-PSK em WLAN 1, verifique a caixa de verificação **permitida** ao lado da chave pré-compartilhada na área de parâmetros WPA e entre na frase de passagem para o WPA-PSK. O WPA-PSK usará o TKIP para a criptografia. **Nota:** A frase de passagem WPA-PSK deve combinar a frase de passagem que é configurada no adaptador cliente para que o WPA-PSK trabalhe. Clique em Apply. Aqui está um exemplo:



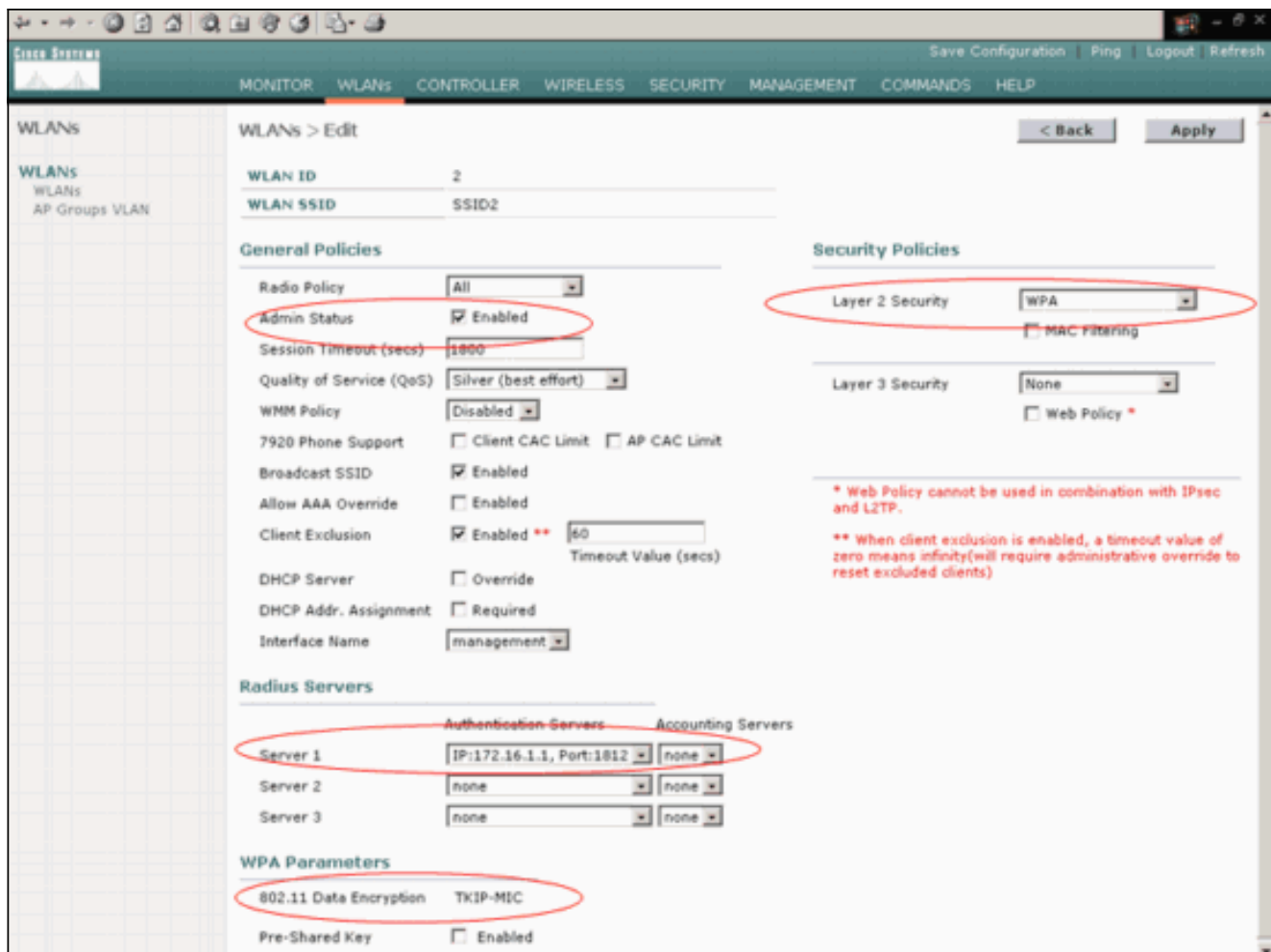
Você configurou WLAN 1 para a criptografia WPA-PSK.

4. A fim definir WLAN 2, clique **novo** na janela WLANs. O WLAN > a nova janela aparecem.
5. No o WLAN > a nova janela, definem o ID de WLAN e o WLAN SSID, e o clique **aplica-se**. Aqui está um exemplo:



O WLAN > edita o indicador para o segundo WLAN aparece.

6. Faça estas seleções no WLAN > para editar o indicador: Na área de políticas gerais, verifique a caixa de verificação **permitida** ao lado do status administrativo a fim permitir este WLAN. Escolha o **WPA** do menu suspenso da Segurança da camada 2 a fim configurar o WPA para este WLAN. Na área dos servidores Radius, escolha o servidor Radius apropriado usar-se para a autenticação dos clientes. Clique em Apply. Aqui está um exemplo:



Nota: Este original não explica como configurar os servidores Radius e a autenticação de EAP. Para obter informações sobre de como configurar a autenticação de EAP com WLC, refira a [autenticação de EAP com exemplo de configuração dos controladores de WLAN \(WLC\)](#).

[Apronte o AP para a instalação no local remoto](#)

A escorva é um processo por que os regaços obtêm uma lista de controladores a que podem conectar. Os regaços estão informados de todos os controladores no grupo da mobilidade assim que conectarem a um único controlador. Desta maneira, os regaços aprendem toda a informação que precisam a fim se juntar a todo o controlador no grupo.

A fim aprontar um AP Colher-capaz, conecte o AP à rede ligada com fio no escritório principal. Esta conexão permite que o AP descubra um único controlador. Depois que o REGAÇO se junta ao controlador no escritório principal, o AP transfere a versão do operating system (OS) AP que corresponde com o infra-estrutura WLAN e a configuração. Os endereços IP de Um ou Mais Servidores Cisco ICM NT de todos os controladores no grupo da mobilidade são transferidos ao AP. Quando o AP tem toda a informação que precisa, o AP pode ser conectado na posição remota. O AP pode então descobrir e juntar-se ao controlador menos-utilizado da lista, se a conectividade IP está disponível.

Nota: Certifique-se de que você ajusta os AP "COLHE" o modo antes que você os desligue a fim os enviar aos locais remotos. Você pode ajustar o modo a nível AP através do controlador CLI ou GUI, ou com o uso de moldes wireless do sistema de controle (WCS). Os AP são ajustados para executar à revelia o regular, funcionalidade "local".

Os regaços podem usar qualquer destes métodos a fim descobrir o controlador:

- **Descoberta da camada 2**
- **Descoberta da camada 3** Com o uso de uma transmissão da sub-rede local Com o uso da opção de DHCP 43 Com o uso de um servidor DNS Com o uso sobre do - Abastecimento do ar (OTAP) Com o uso de um servidor DHCP interno **Nota:** A fim usar um servidor DHCP interno, o REGAÇO deve conectar diretamente ao WLC.

Este original supõe que o REGAÇO se registra ao WLC com uso do mecanismo de descoberta da opção de DHCP 43. Para obter mais informações sobre do uso da opção de DHCP 43 registrar o REGAÇO ao controlador, assim como dos outros mecanismos de descoberta, refere o [registro de pouco peso AP \(REGAÇO\) a um controlador do Wireless LAN \(WLC\)](#).

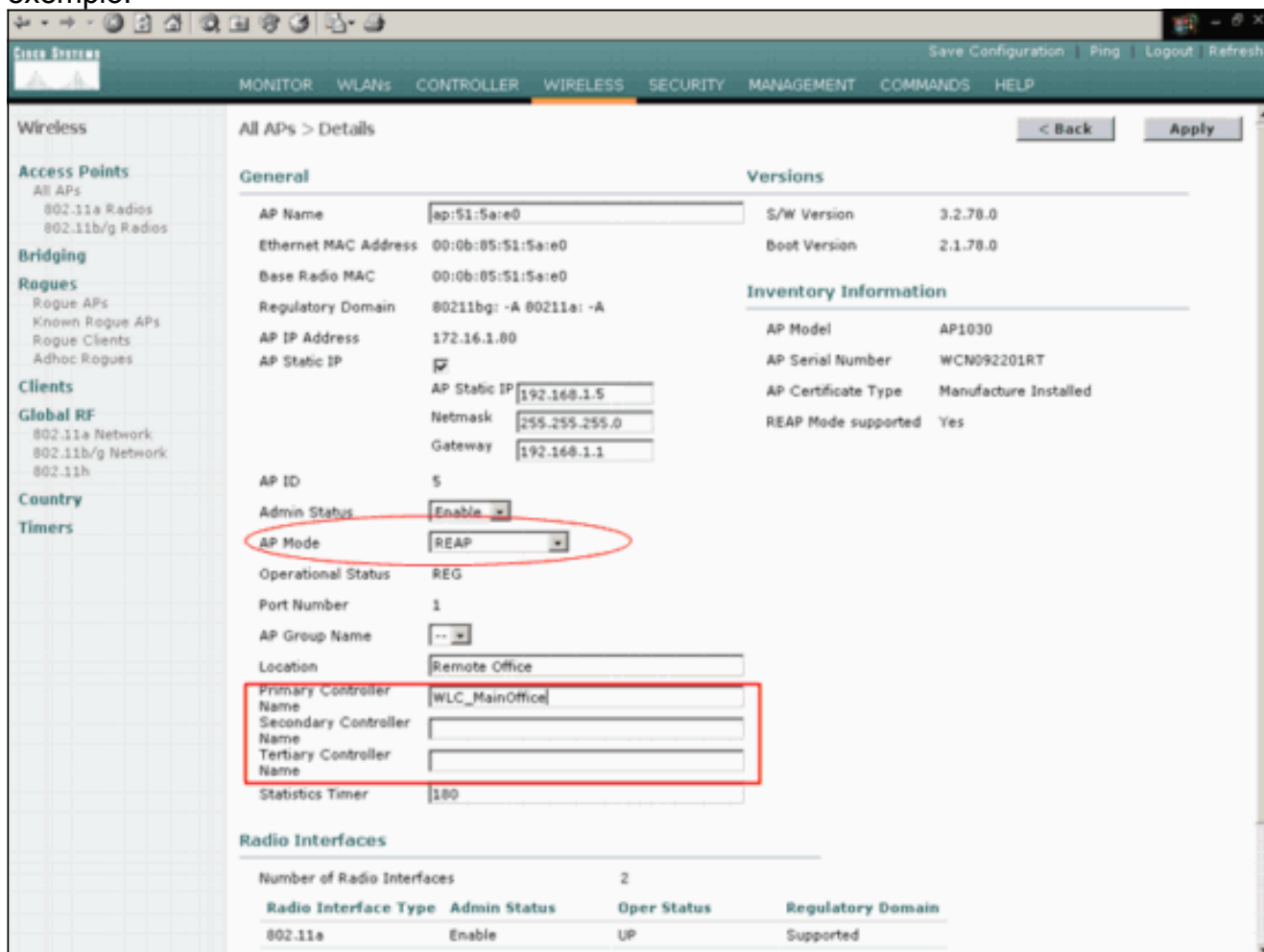
Depois que o REGAÇO descobre o controlador, você pode ver que o AP está registrado ao controlador na janela wireless do WLC. Aqui está um exemplo:

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:51:5a:e0	5	00:0b:05:51:5a:e0	Enable	REG	1	Detail

Termine estas etapas a fim configurar o REGAÇO para o modo normal REAP:

1. Na GUI da WLC, clique em **Wireless**. Toda a janela APS aparece. Este indicador alista os AP que são registrados ao WLC.
2. Selecione o AP que você deve configurar para o modo REAP e clicar o **detalhe**. O todo o indicador AP > de detalhe para o AP específico aparece. Neste indicador, você pode configurar os vários parâmetros do AP, que incluem: Nome AP Endereço IP de Um ou Mais Servidores Cisco ICM NT (que você pode mudar à estática) Status administrativo Parâmetros de segurança Modo AP Lista de WLC a que o AP pode conectar Outros parâmetros
3. Escolha **COLHEM do** menu suspenso do modo AP. Este modo está somente disponível em AP Colher-capazes.

4. Defina os nomes do controlador que os AP se usarão para registrar e o clique **aplica-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. Aqui está um exemplo:



Você estabeleceu o AP para o modo REAP, e você pode distribuí-lo no local remoto.

Nota: Neste exemplo de janela, você pode ver que o endereço IP de Um ou Mais Servidores Cisco ICM NT do AP está mudado à estática e um endereço IP estático 192.168.1.5 está atribuído. Esta atribuição ocorre porque esta é a sub-rede a ser usada no escritório remoto. Assim você usa o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP, 172.16.1.80, somente durante a fase da escorva. Depois que o AP é registrado ao controlador, você muda o endereço a um endereço IP estático.

[Configurar os 2800 Router para estabelecer o link MACILENTO](#)

A fim estabelecer o link MACILENTO, este exemplo usa dois 2800 Series Router com o OSPF à informação de rota entre as redes. Está aqui a configuração de ambo o Roteadores para o exemplo de cenário neste original:

```
MainOffice
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-Templatel 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
```

BranchOffice

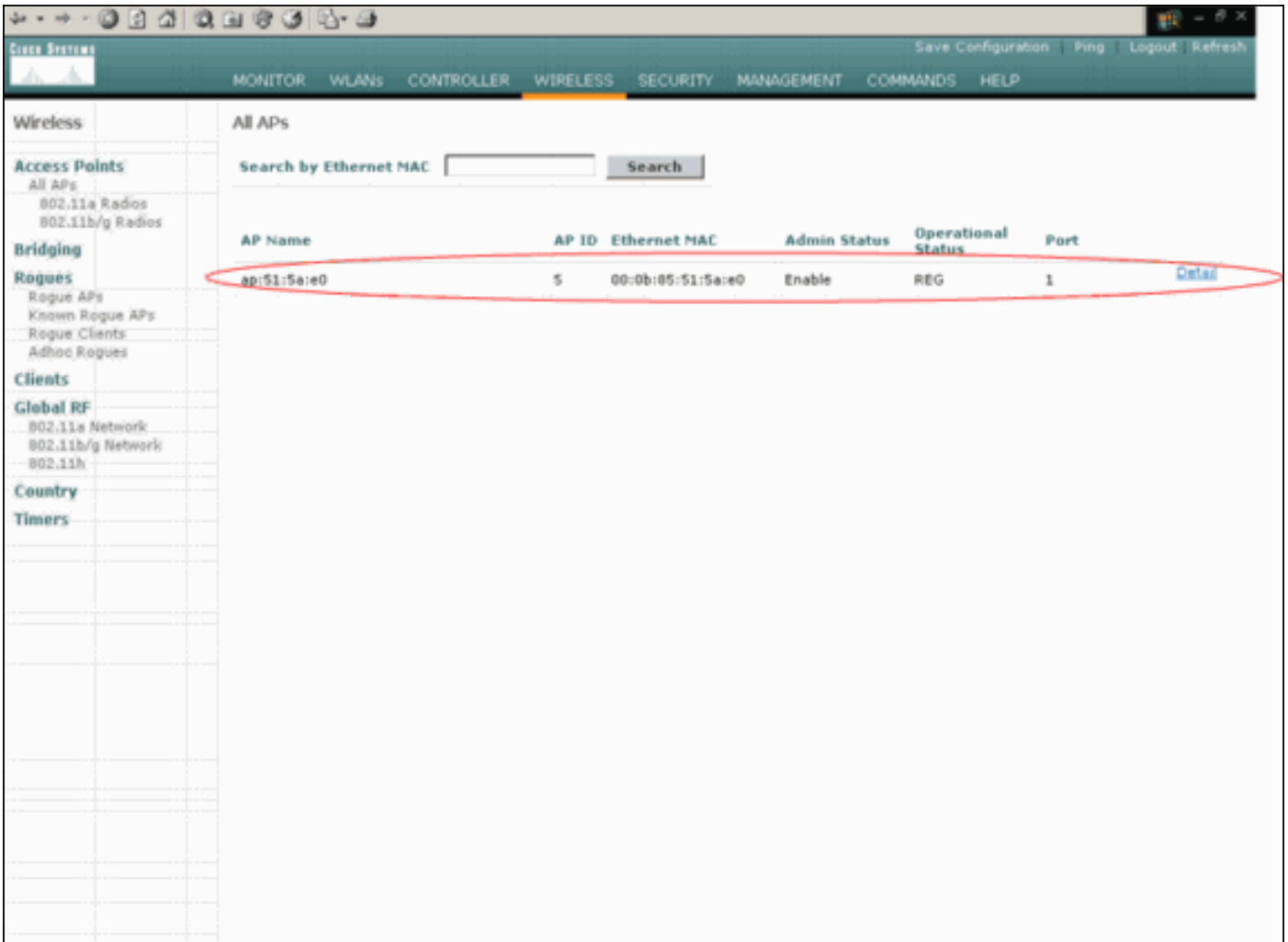
```
BranchOffice#show run
Building configuration...

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
```

Distribua a COLHEITA AP no local remoto

Agora que você configurou WLAN nos WLC, os aprontou o REGAÇO, e os estabeleceu o link MACILENTO entre o escritório principal e o escritório remoto, você está pronto para distribuir o AP no local remoto.

Depois que você põe acima o AP no local remoto, o AP procura o controlador na ordem que você configurou na fase da escorva. Depois que o AP encontra o controlador, o AP registra-se com o controlador. Exemplo: Do WLC, você pode ver que o AP se juntou ao controlador na porta 1:



AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:51:5a:e0	5	00:0b:05:51:5a:e0	Enable	REG	1	Detail

Clientes que têm o SSID **SSID1**, e para que WPA-PSK é permitido, associado ao AP nos clientes WLAN 1. que têm o SSID **SSID2**, e que têm a autenticação do 802.1x permitida, associado ao AP em WLAN 2. Está aqui um exemplo que mostre dois clientes. Um cliente é conectado a WLAN 1, e o outro cliente é conectado a WLAN 2:

Save Configuration Ping Logout Ref Close

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor Clients Items 1 to 2 of 2

Search by MAC address Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:dd:05	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID1	802.11a	Associated	Yes	1	Detail Link Test Disable Remove
00:40:96:ac:e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	Detail Link Test Disable Remove

Summary
Statistics
Controller Ports
Wireless
Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues
802.11a Radios
802.11b/g Radios
Clients
RADIUS Servers

Verificar

Use esta seção para confirmar que seu COLHA trabalhos da configuração corretamente.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Derrube o link MACILENTO. Quando o link MACILENTO está para baixo, o AP perde a Conectividade com o WLC. O WLC cancela a matrícula então o AP de sua lista. Aqui está um exemplo:

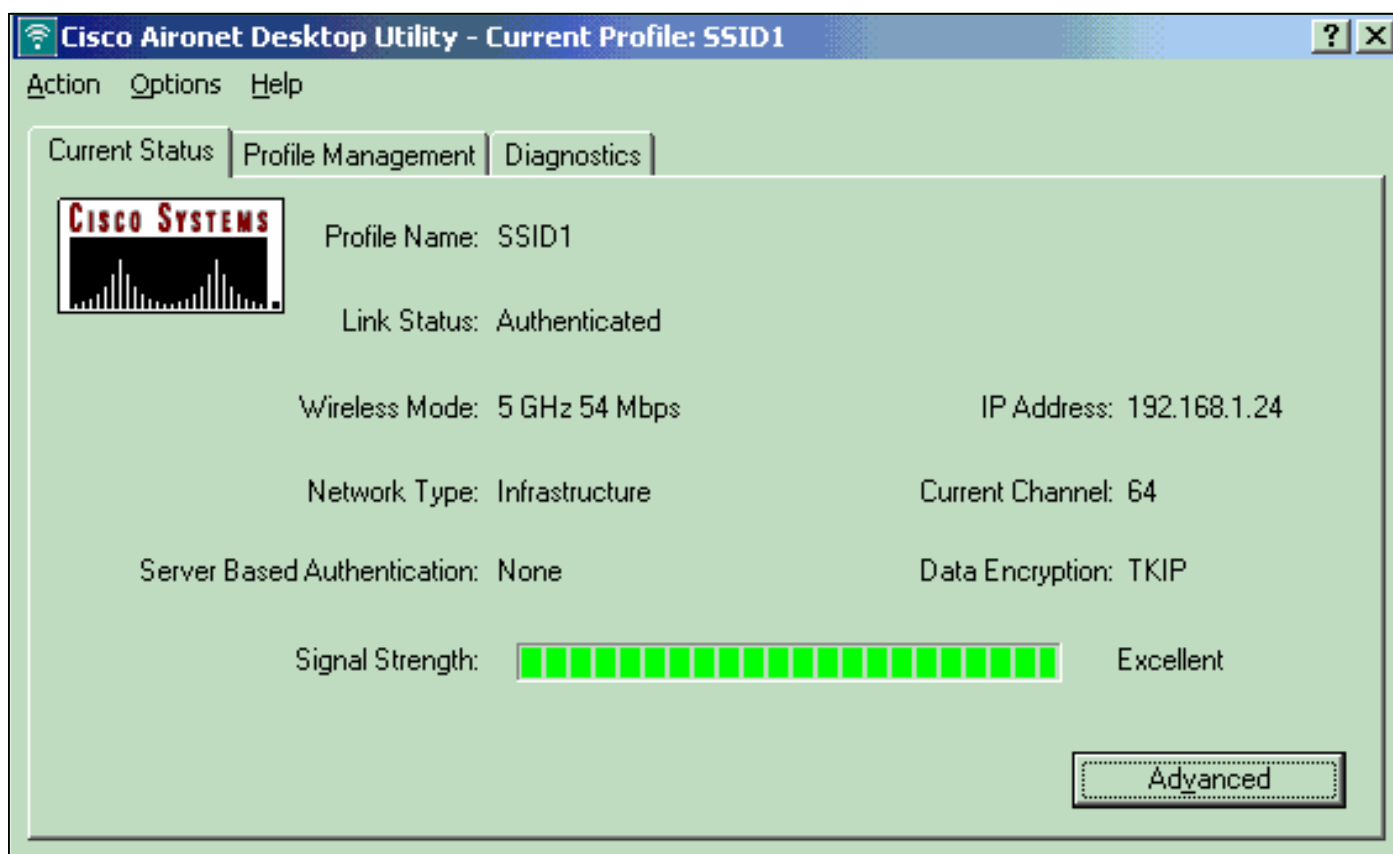
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: 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
```

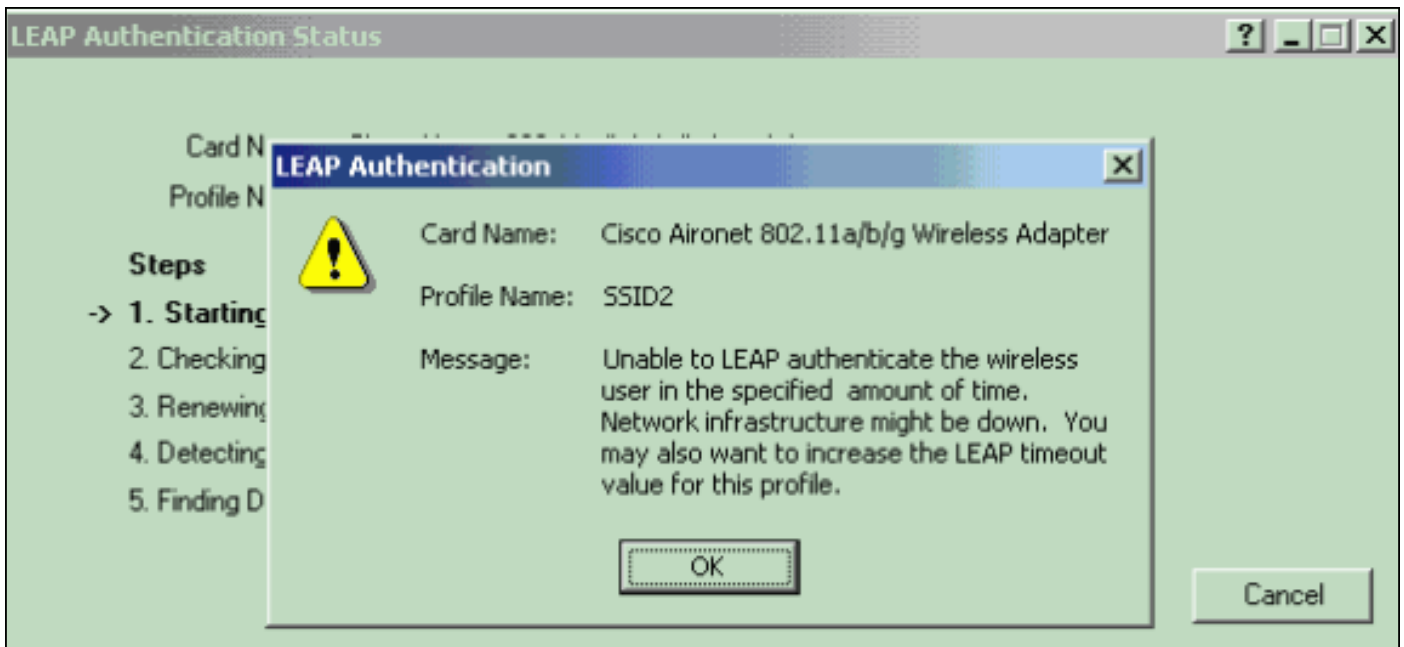
Da saída do comando **debug lwapp events enable**, você pode ver que o WLC cancela a matrícula o AP porque o WLC não recebeu uma resposta da pulsação do coração do AP. Uma resposta da pulsação do coração é similar aos mensagens de keepalive. O controlador tenta cinco heartbeats consecutiva, 1 segundo separado. Se o WLC não recebe uma resposta, o WLC cancela a matrícula o AP.

Quando o AP reage do modo independente, o diodo emissor de luz da potência AP pisca. Os clientes que associam ao primeiro WLAN (WLAN 1) são associados ainda ao AP porque os clientes no primeiro WLAN são configurados para a criptografia WPA-PSK somente. O REGAÇO segura a criptografia própria no modo independente. Está aqui um exemplo que mostre o estado (quando o link MACILENTO está para baixo) de um cliente que seja conectado a WLAN 1 com o SSID1 e o WPA-PSK:

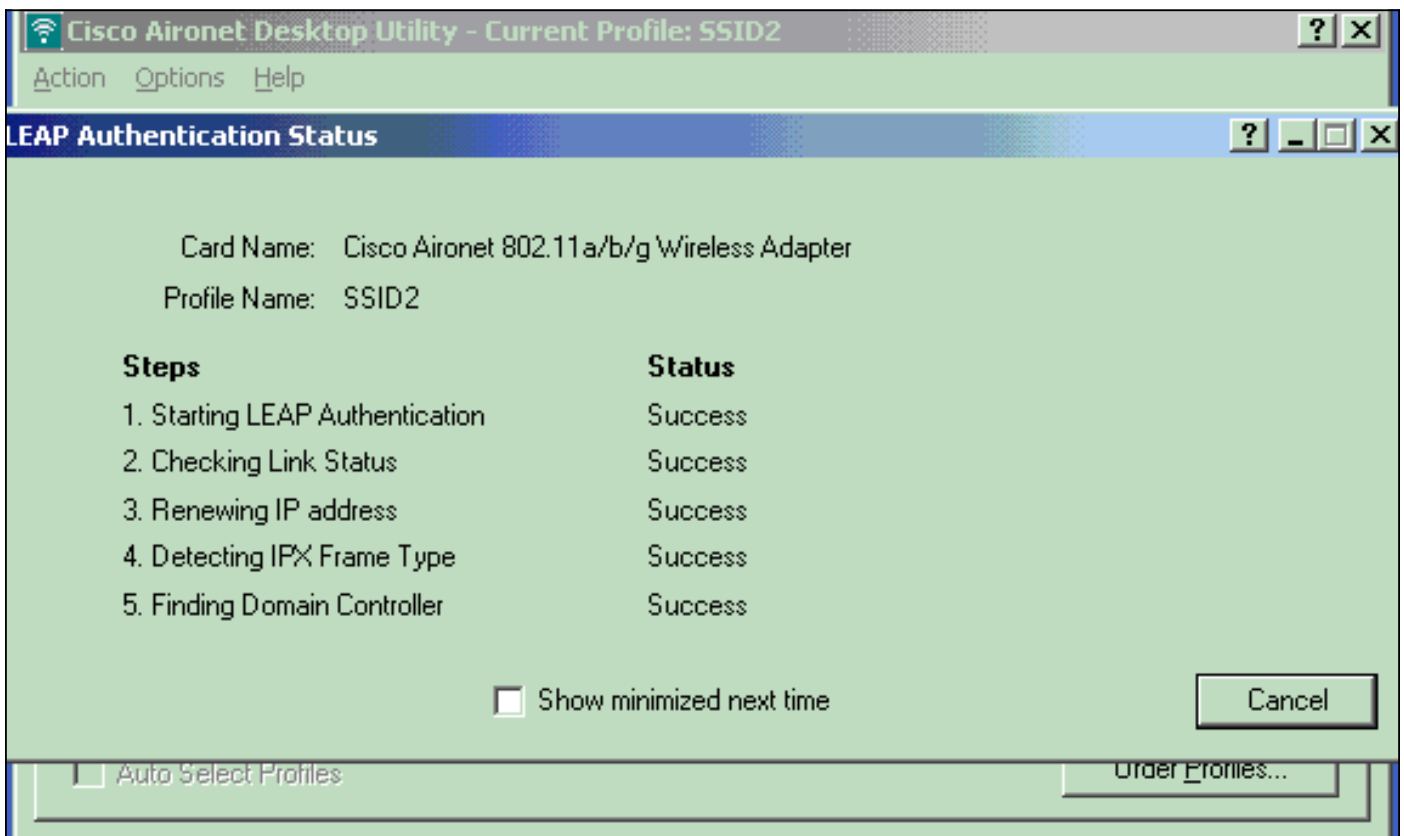
Nota: O TKIP é a criptografia que é usada com WPA-PSK.



Os clientes que são conectados a WLAN 2 são desligados porque o WLAN 2 usa a autenticação de EAP. Esta desconexão ocorre porque os clientes que usam a necessidade da autenticação de EAP de se comunicar ao WLC. Está aqui um exemplo de janela que mostre que a autenticação de EAP falha quando o link MACILENTO está para baixo:



Depois que o link MACILENTO está acima, o AP comuta de volta ao modo normal REAP e registra-se com o controlador. O cliente que usa a autenticação de EAP igualmente vem acima. 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
```

[Troubleshooting](#)

Use esta seção para resolver problemas de configuração.

[Comandos para Troubleshooting](#)

Você pode usar estes **comandos debug** pesquisar defeitos a configuração.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debugar eventos do lwapp permitem** — Indica a sequência de evento que ocorre entre o REGAÇO e o WLC.
- **debugar erros de lwapp permitem** — Indica os erros que ocorrem na comunicação LWAPP.
- **debugar o pacote lwapp permitem** — Indica debugar de um traço do pacote lwapp.
- **debugar o ADDR do Mac** — Permite a eliminação de erros MAC para o cliente que você especifica.

[Informações Relacionadas](#)

- [COLHA o guia de distribuição no escritório filial](#)
- [Autenticação de EAP com exemplo de configuração dos controladores de WLAN \(WLC\)](#)
- [Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight](#)
- [Failover do controlador de WLAN para o exemplo de configuração do Lightweight Access Points](#)
- [Página de Suporte Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)