Convidado WLAN e WLAN interno usando o exemplo de configuração WLC

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Instalação de rede
Configurar
Configurar interfaces dinâmica no WLC para o convidado e os usuários internos
Crie WLAN para o convidado e os usuários internos
Configurar a porta do switch de Camada 2 que conecta ao WLC como a porta de tronco
Configurar o roteador para os dois WLAN
Verificar
Troubleshooting
Procedimento de Troubleshooting
Comandos para Troubleshooting
Informações Relacionadas

Introdução

Este documento fornece um exemplo de configuração para um LAN Wireless (WLAN) de convidado e uma WLAN interna segura que usa Controllers de LAN Wireless (WLCs) e lightweight access points (LAPs) Na configuração neste documento, a WLAN convidada usa a autenticação web para autenticar usuários e a WLAN interna segura usa a autenticação Extensible Authentication Protocol (EAP).

Pré-requisitos

Requisitos

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

- Conhecimento de como configurar o WLC com parâmetros básicos
- Conhecimento de como estabelecer um server DHCP e de Domain Name System (DNS)

Componentes Utilizados

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

- Cisco 2006 WLC que executa a versão de firmware 4.0
- REGAÇO do Cisco 1000 Series
- Adaptador de cliente Wireless de Cisco 802.11a/b/g que executa a versão de firmware 2.6
- Cisco 2811 Router que executa a versão 12.4(2)XA de Cisco IOS®
- 3500 XL series switch de Cisco que executam a versão do Cisco IOS 12.0(5)WC3b
- Servidor DNS que é executado em um Servidor do Microsoft Windows 2000

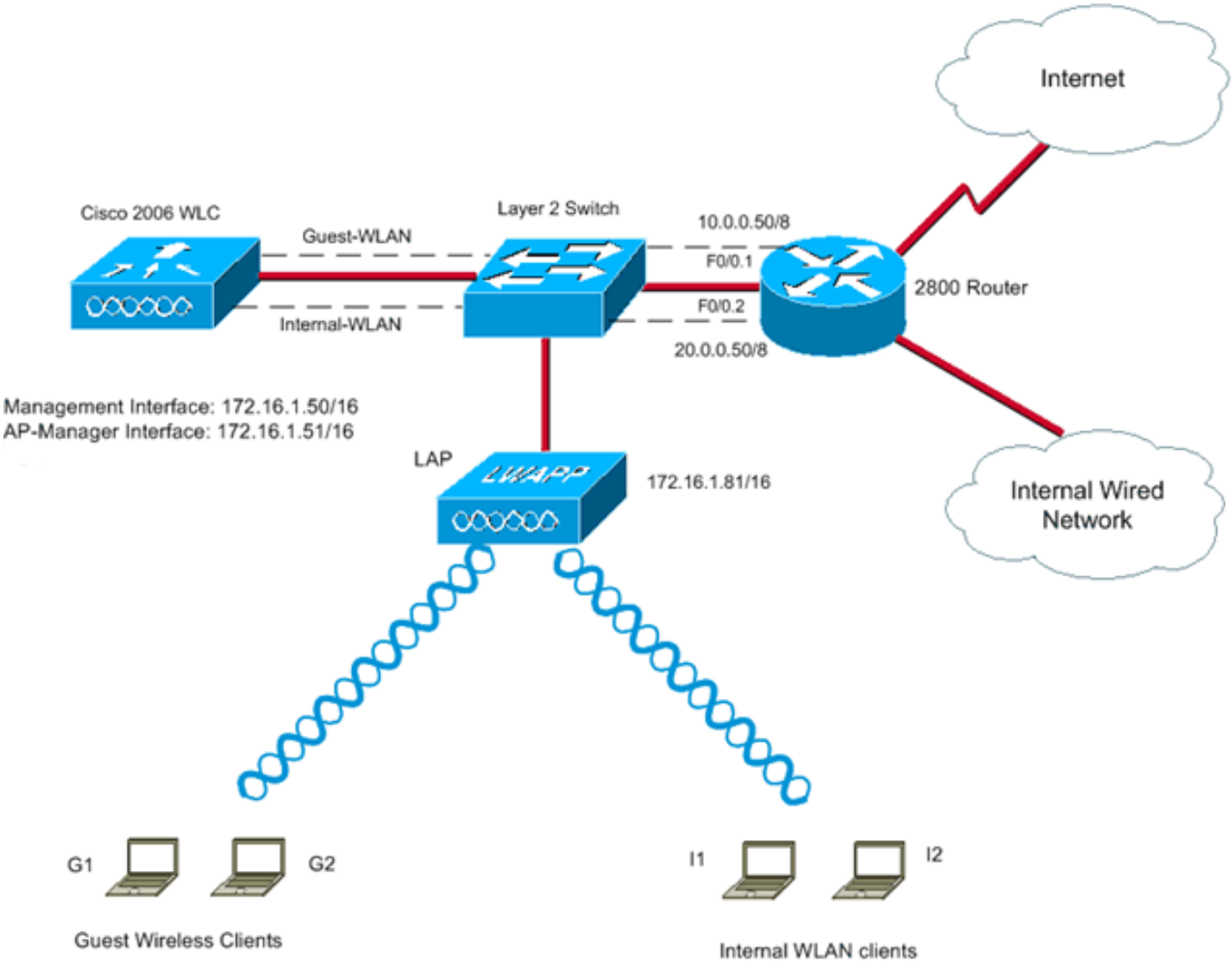
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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

Convenções

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

Instalação de rede

O exemplo de configuração neste documento usa a instalação indicada neste diagrama. O REGAÇO é registrado ao WLC. O WLC é conectado ao switch de Camada 2. O roteador que conecta os usuários a WAN igualmente conecta ao switch de Camada 2. Você precisa de criar dois WLAN, um para os usuários convidado e o outro para os usuários da LAN interna. Você igualmente precisa um servidor DHCP de fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT para o convidado e os clientes Wireless internos. Os usuários convidado usam a autenticação da Web a fim alcançar a rede. Os usuários internos usam a autenticação de EAP. O 2811 Router igualmente atua como o servidor DHCP para os clientes Wireless.



Nota: Este documento supõe que o WLC está configurado com os parâmetros básicos e o REGAÇO está registrado ao WLC. Refira o registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (WLC) para obter informações sobre de como configurar os parâmetros básicos em um WLC e de como registrar o REGAÇO ao WLC.

Quando configurados como um servidor DHCP, alguns dos Firewall não apoiam requisições DHCP de um agente de transmissão. O WLC é um agente de transmissão para o cliente. O Firewall configurado como um servidor DHCP ignora estes pedidos. Os clientes devem diretamente ser conectados ao Firewall e não podem enviar pedidos através de um outro agente de transmissão ou roteador. O Firewall pode trabalhar como um servidor DHCP simples para os host internos que lhe são conectados diretamente. Isto permite que o Firewall mantenha sua tabela baseada nos endereços MAC que são conectados diretamente e que pode ver. Eis porque uma tentativa de atribuir endereços de uma transmissão de DHCP não está disponível e os pacotes são rejeitados. O PIX Firewall tem esta limitação.

Configurar

Termine estas etapas a fim configurar os dispositivos para esta instalação de rede:

1. Configurar interfaces dinâmica no WLC para o convidado e os usuários internos
2. Crie WLAN para o convidado e os usuários internos
3. Configurar a porta do switch de Camada 2 que conecta ao WLC como a porta de tronco

4. Configurar o roteador para os dois VLAN

Configurar interfaces dinâmica no WLC para o convidado e os usuários internos

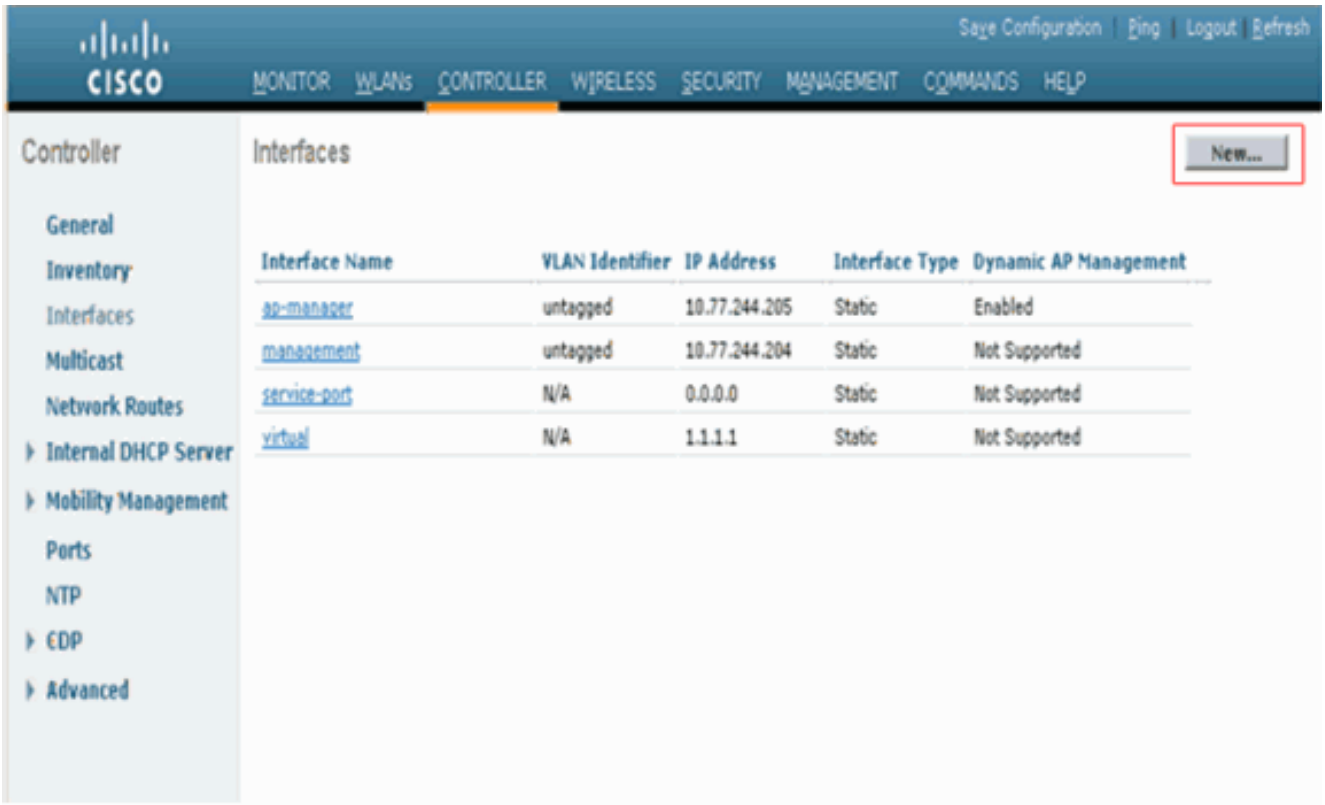
A primeira etapa é criar duas interfaces dinâmica no WLC, em um para os usuários convidado e no outro para usuários internos.

O exemplo neste documento usa estes parâmetros e valores para as interfaces dinâmica:

```
Guest-WLAN                                          Internal-WLAN
VLAN Id : 10                          VLAN Id : 20
IP address: 10.0.0.10                    IP address: 20.0.0.10
Netmask: 255.0.0.0 Netmask: 255.0.0.0
Gateway: 10.0.0.50                       Gateway: 20.0.0.50
Physical port on WLC: 1                     Physical port on WLC: 1
DHCP server: 172.16.1.60                      DHCP server: 172.16.1.60
```

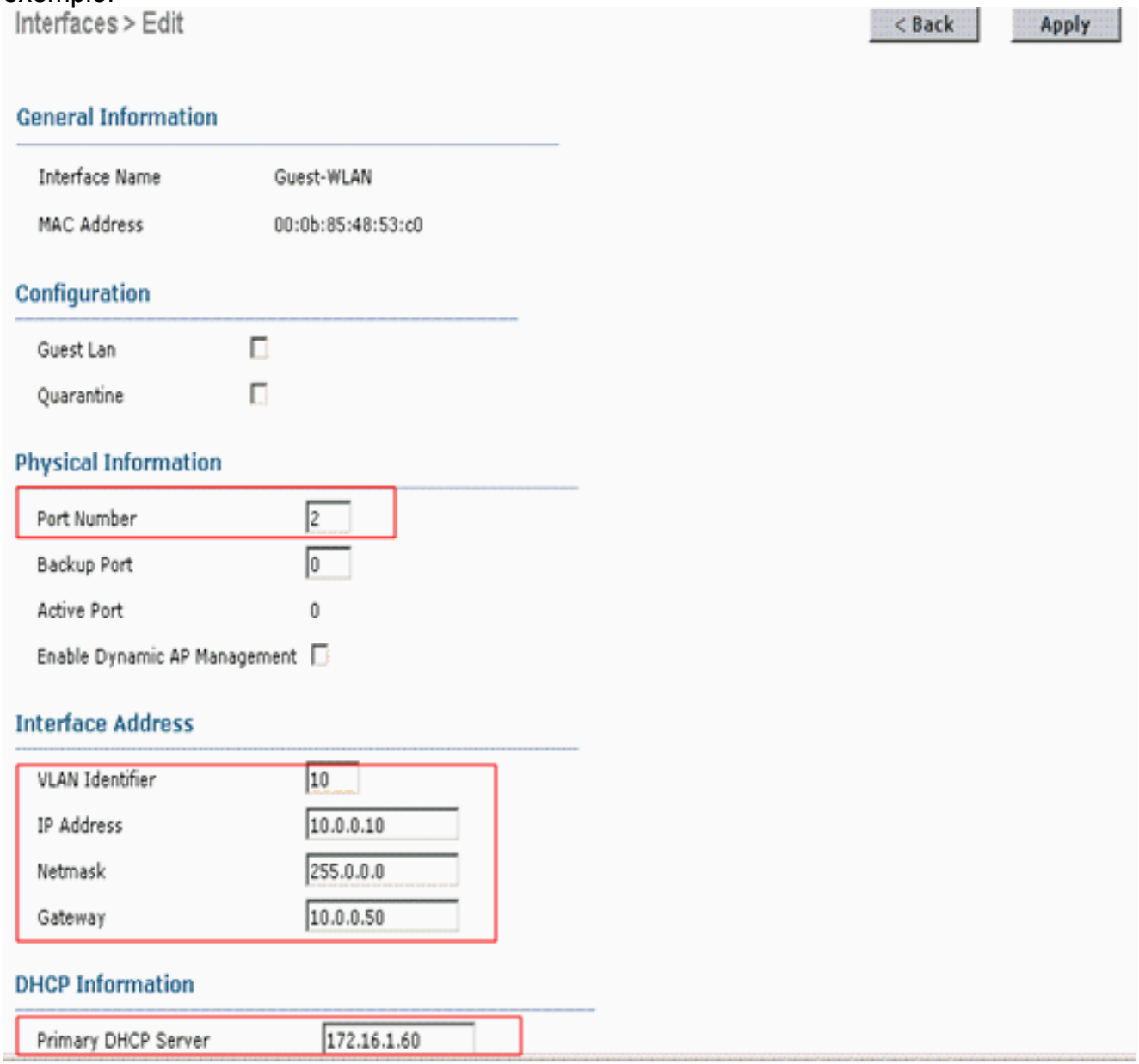
Conclua estes passos:

1. Do WLC GUI, escolha **controladores > relações**.O indicador das relações aparece. Este indicador alista as relações que são configuradas no controlador. Isto inclui as interfaces padrão, que são a interface de gerenciamento, relação do ap-gerente, a interface virtual e a interface de porta do serviço, e as interfaces dinâmica definidas pelo utilizador.



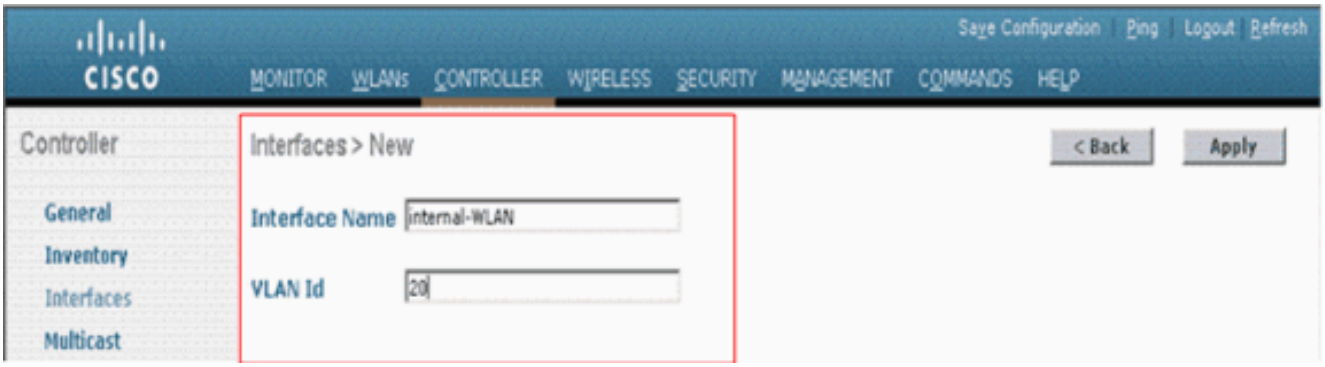
2. Clique **novo** a fim criar uma interface dinâmica nova.
3. Nas relações > na nova janela, incorpore o nome da relação e a identificação VLAN. Então, o clique **aplica-se**.Neste exemplo, a interface dinâmica é nomeada Convidado-WLAN e a identificação VLAN é atribuída o
10.

4. Nas relações > edite o indicador, para a interface dinâmica, entre no endereço IP de Um ou Mais Servidores Cisco ICM NT, na máscara de sub-rede, e no gateway padrão. Atribua-à uma porta física no WLC, e incorpore-o o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP. Então, o clique **aplica-se**.Este é o exemplo:

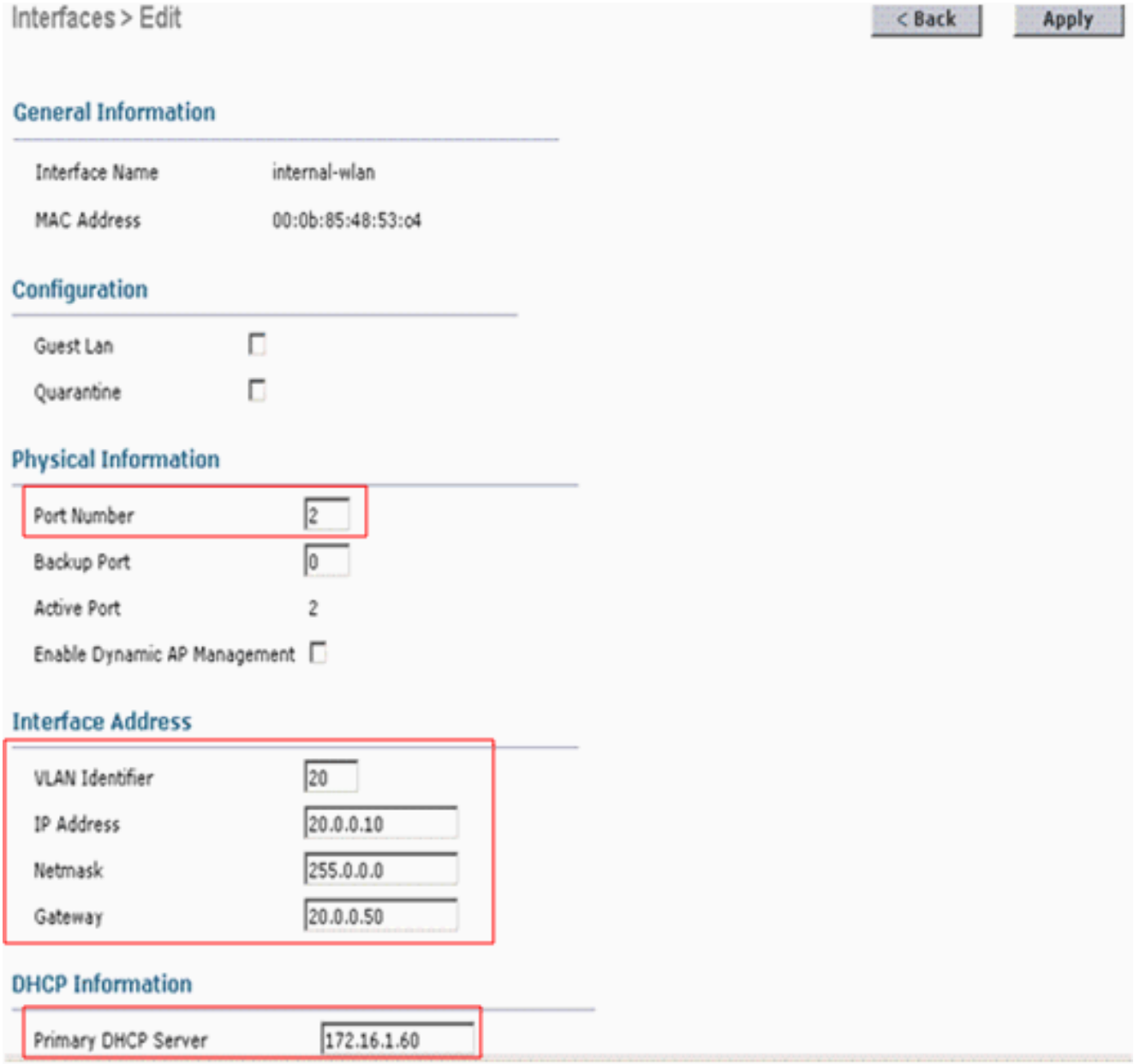


O mesmo procedimento deve ser terminado a fim criar uma interface dinâmica para o WLAN interno.

5. Nas relações > na nova janela, incorpore o Interno-**WLAN** para a interface dinâmica para os usuários internos, e incorpore **20** para a identificação VLAN. Então, o clique **aplica-se**.



6. Nas relações > edite o indicador, para a interface dinâmica, entre no endereço IP de Um ou Mais Servidores Cisco ICM NT, na máscara de sub-rede, e no gateway padrão. Atribua-à uma porta física no WLC, e incorpore-o o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP. Então, o clique **aplica-se**.



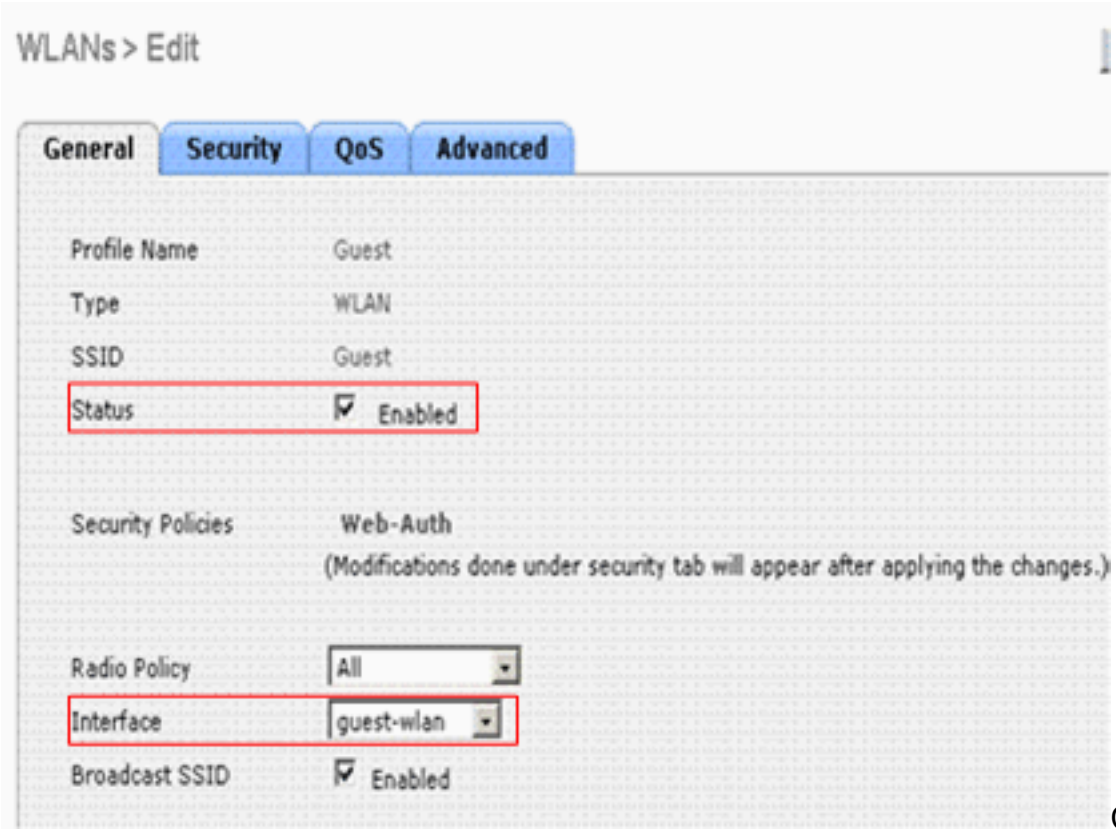
Agora que duas interfaces dinâmica são criadas, o indicador das relações resume a lista de relações configuradas no
controlador.

Crie WLAN para o convidado e os usuários internos

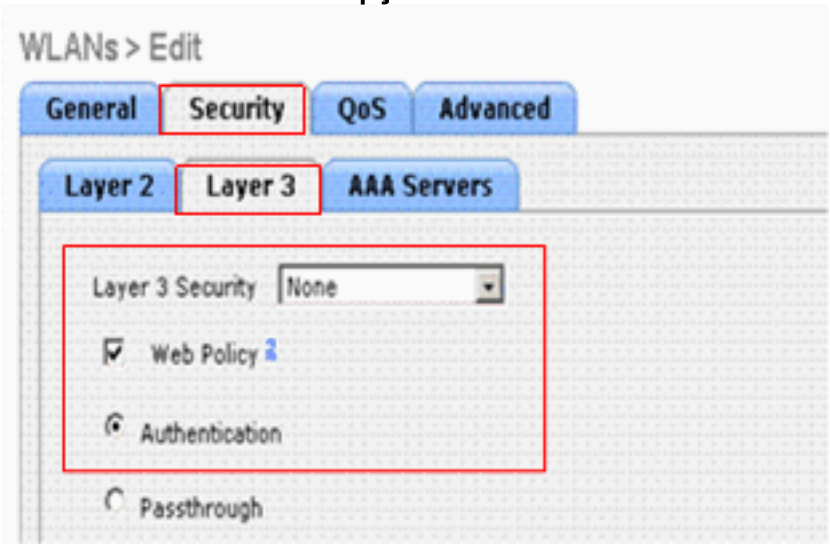
A próxima etapa é criar WLAN para os usuários convidado e os usuários internos, e traça a interface dinâmica aos WLAN. Também, os métodos de segurança que são usados para autenticar o convidado e os usuários Wireless devem ser definidos. Conclua estes passos:

1. Clique **WLAN do** controlador GUI a fim criar um WLAN.A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo.Neste exemplo, o WLAN é nomeado *Convidado* e o ID de WLAN é

2.
3. O clique **aplica-se no** canto superior direito.
4. O WLAN > edita a tela aparece, que contém várias abas.Sob o **tab geral** para o convidado WLAN, escolha o convidado-**WLAN do** campo de nome da relação. Isto traça a interface dinâmica convidado-**WLAN** que foi criada previamente ao **convidado** WLAN.Certifique-se de que o estado do WLAN está

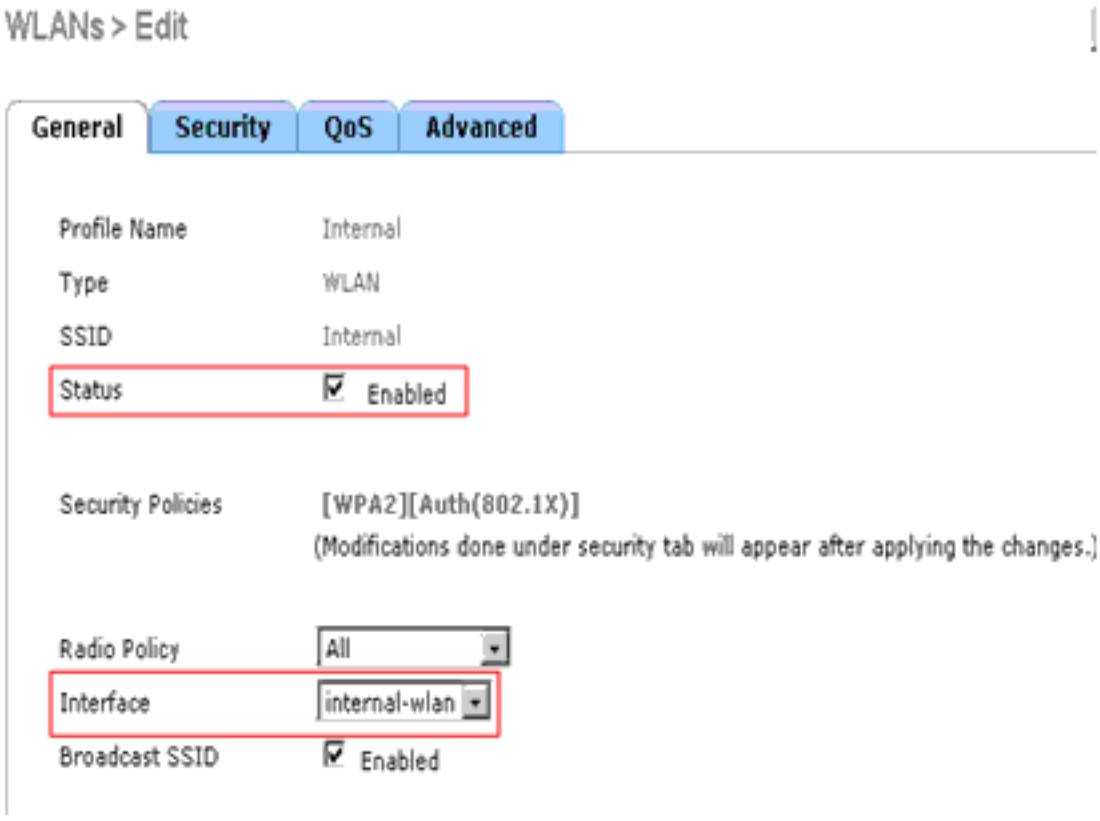


permitido. Cliq ue na guia Security. Para este WLAN, a autenticação da Web um mecanismo de segurança da camada 3 é usada para autenticar clientes. , Não escolha consequentemente **nenhuns** sob o campo de Segurança da *camada 2*. No campo de Segurança da *camada 3*, verifique a caixa da **política da Web** e escolha a **opção de**

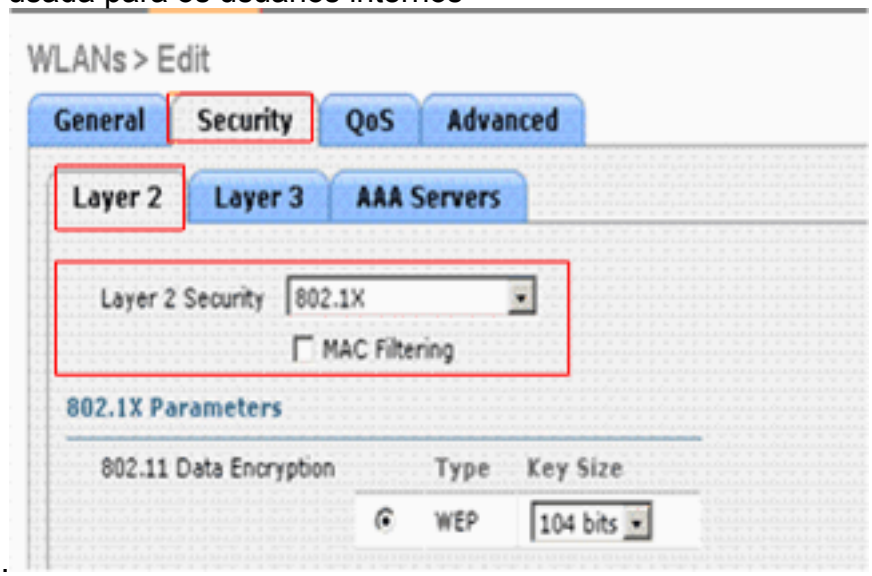


autenticação. **Nota:** Para obter mais informações sobre da autenticação da Web, refira o [exemplo de configuração da autenticação da Web do controlador do Wireless LAN](#).Clique em Apply.

5. Crie um WLAN para os usuários internos. No os WLAN > a nova janela, entram em **interno** e escolhem **3** a fim criar um WLAN para os usuários internos. Então, o clique **aplica-se**.
6. Os WLAN > editam o indicador aparecem. Sob o *tab geral*, escolha o interno-**WLAN do** campo de nome da relação.Isto traça a interface dinâmica interno-**WLAN** que foi criada previamente ao WLAN **interno**. Certifique-se de que o WLAN está



permitido. Deixe a opção de segurança da camada 2 no 802.1x do valor padrão porque a autenticação de EAP é usada para os usuários internos



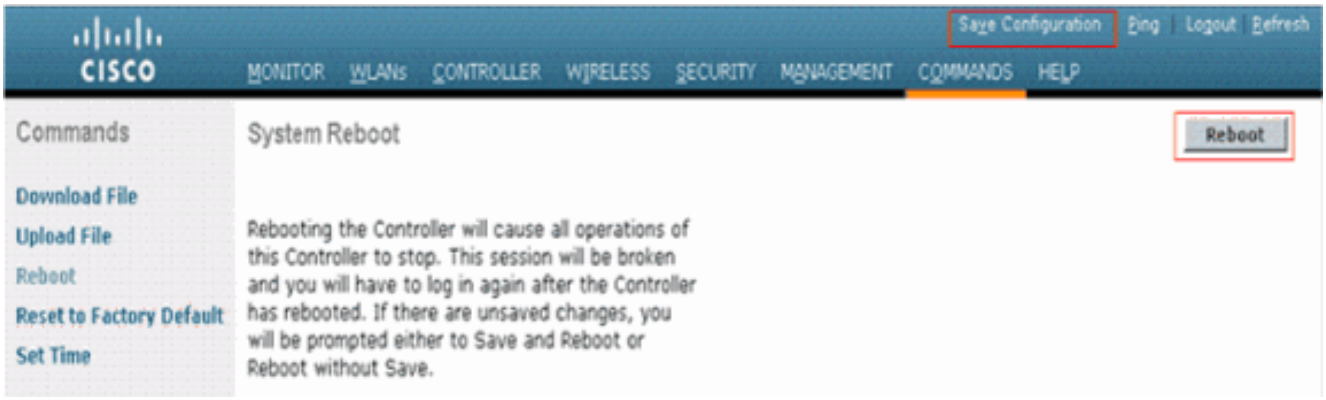
WLAN.

7. Clique em Apply.O indicador WLAN aparece e mostra a lista de WLAN que são criados.

Nota: Refira a autenticação de EAP com exemplo de configuração dos controladores de WLAN (WLC) para informações mais detalhadas sobre de como configurar um WLAN EAP-

baseado com WLC.

8. No WLC GUI, clique a **configuração da salvaguarda**, a seguir clique **comandos do** controlador GUI. Em seguida, escolha a opção da **repartição** recarregar o WLC a fim permitir que a autenticação da Web tome o efeito.



Nota: Configuração da salvaguarda do clique a fim salvar a configuração através das repartições.

Configurar a porta do switch de Camada 2 que conecta ao WLC como a porta de tronco

Você precisa de configurar a porta de switch para apoiar os vlan múltiplos configurados no WLC porque o WLC é conectado a um switch de Camada 2. Você deve configurar a porta de switch como uma porta de tronco 802.1Q.

Cada conexão de porta do controlador é um tronco 802.1Q e deve ser configurada como este no switch vizinho. Em switch Cisco, o VLAN nativo de um tronco 802.1Q, por exemplo **VLAN1**, é deixado o sem etiqueta. Consequentemente, se você configura a relação de um controlador para usar o VLAN nativo em um switch Cisco vizinho, certifique-se de você configurar a relação no controlador como o sem etiqueta.

Um valor zero para o **identificador de VLAN** (no controlador > conecta o indicador) significa que a relação é sem etiqueta. No exemplo neste documento, o gerenciador AP e as interfaces de gerenciamento são configurados no VLAN sem etiqueta do padrão.

Quando uma relação do controlador é ajustada a um valor diferente de zero, não deve ser etiquetada ao VLAN nativo do interruptor e o VLAN deve ser permitido no interruptor. Neste exemplo, o VLAN 60 é configurado como o VLAN nativo na porta de switch que conecta ao controlador.

Esta é a configuração para a porta de switch que conecta ao WLC:

```
interface f0/12
Description Connected to the WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

Esta é a configuração para a porta de switch que conecta ao roteador como uma porta de tronco:

```
interface f0/10
```

```
Description Connected to the Router
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

Esta é a configuração para a porta de switch que conecta ao REGAÇO. Esta porta é configurada como uma porta de acesso:

```
interface f0/9
Description Connected to the LAP
Switchport access vlan 60
switchport mode access
no ip address
```

Configurar o roteador para os dois WLAN

No exemplo neste documento, o 2811 Router conecta os usuários convidado ao Internet e igualmente conecta os usuários prendidos internos aos usuários Wireless internos. Você igualmente precisa de configurar o roteador para proporcionar serviços DHCP.

No roteador, crie subinterfaces sob a interface fastethernet que conecta à porta de tronco no interruptor para cada VLAN. Atribua as subinterfaces aos VLAN correspondentes, e configurar um endereço IP de Um ou Mais Servidores Cisco ICM NT dos sub-rede respectiva.

Nota: Somente as porções relevantes da configuração de roteador são dadas, e não a configuração completa.

Esta é a configuração exigida no roteador para realizar isto.

Estes são os comandos que devem ser emitidos a fim configurar serviços DHCP no roteador:

```
!
ip dhcp excluded-address 10.0.0.10
!--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC.
ip dhcp excluded-address 10.0.0.50 !--- IP excluded because this IP is assigned to the !--- sub-
interface on the router. ip dhcp excluded-address 20.0.0.10 !--- IP excluded because this IP is
assigned to the dynamic !--- interface created on the WLC. ip dhcp excluded-address 20.0.0.50 !-
-- IP excluded because this IP is assigned to the sub-interface on the router. ! ip dhcp pool
Guest !--- Creates a DHCP pool for the guest users. network 10.0.0.0 255.0.0.0 default-router
10.0.0.50 dns-server 172.16.1.1 !--- Defines the DNS server. ! ip dhcp pool Internal network
20.0.0.0 255.0.0.0 default-router 20.0.0.50 !--- Creates a DHCP pool for the internal users. !
```

Estes comandos devem ser emitidos na interface fastethernet para o exemplo setup:

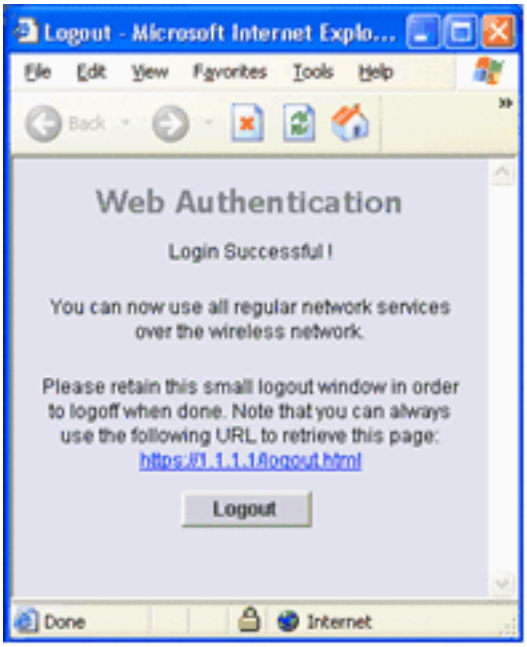
```
!
interface FastEthernet0/0
 description Connected to L2 Switch
 ip address 172.16.1.60 255.255.0.0
 duplex auto
 speed auto
!--- Interface connected to the Layer 2 switch. ! interface FastEthernet0/0.1 description Guest
VLAN encapsulation dot1Q 10 ip address 10.0.0.50 255.0.0.0 !--- Creates a sub-interface under
FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN
encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under
FastEthernet0/0 for the internal VLAN. !
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

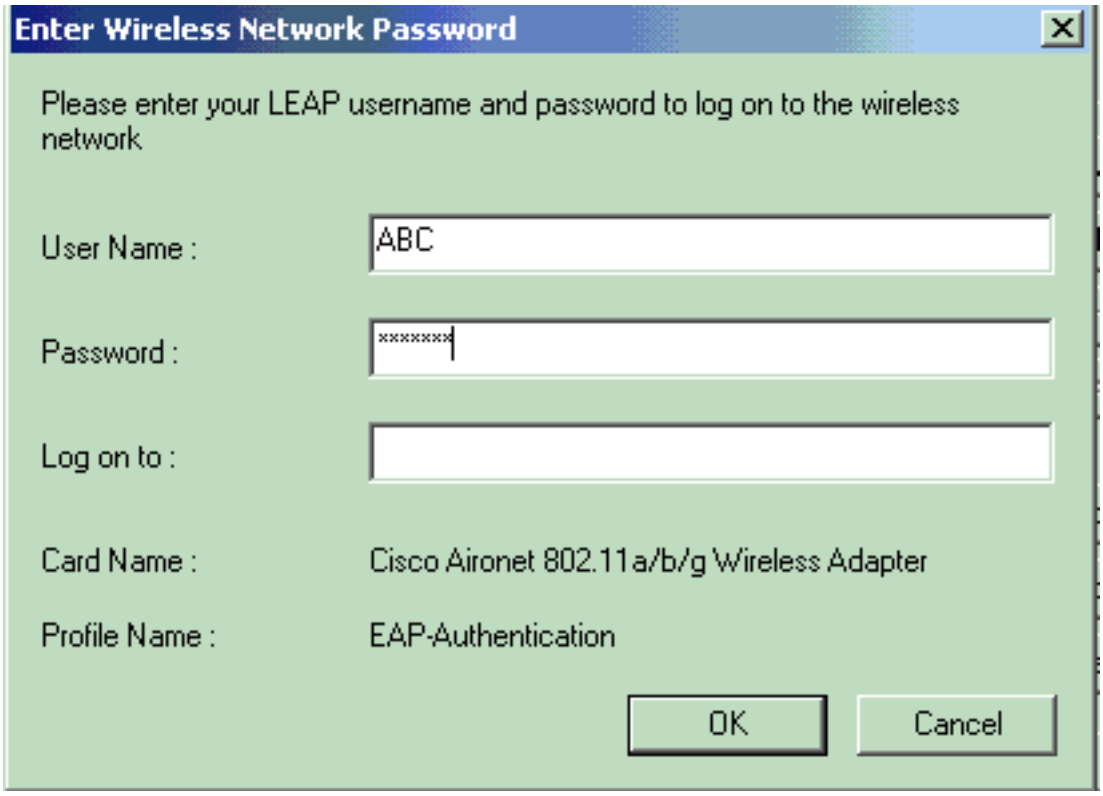
Conecte dois clientes Wireless, um usuário convidado (com o **convidado do** [SSID] do Service Set Identifier) e um usuário interno (com o SSID **interno**), a fim verificar como esperado os trabalhos da configuração.

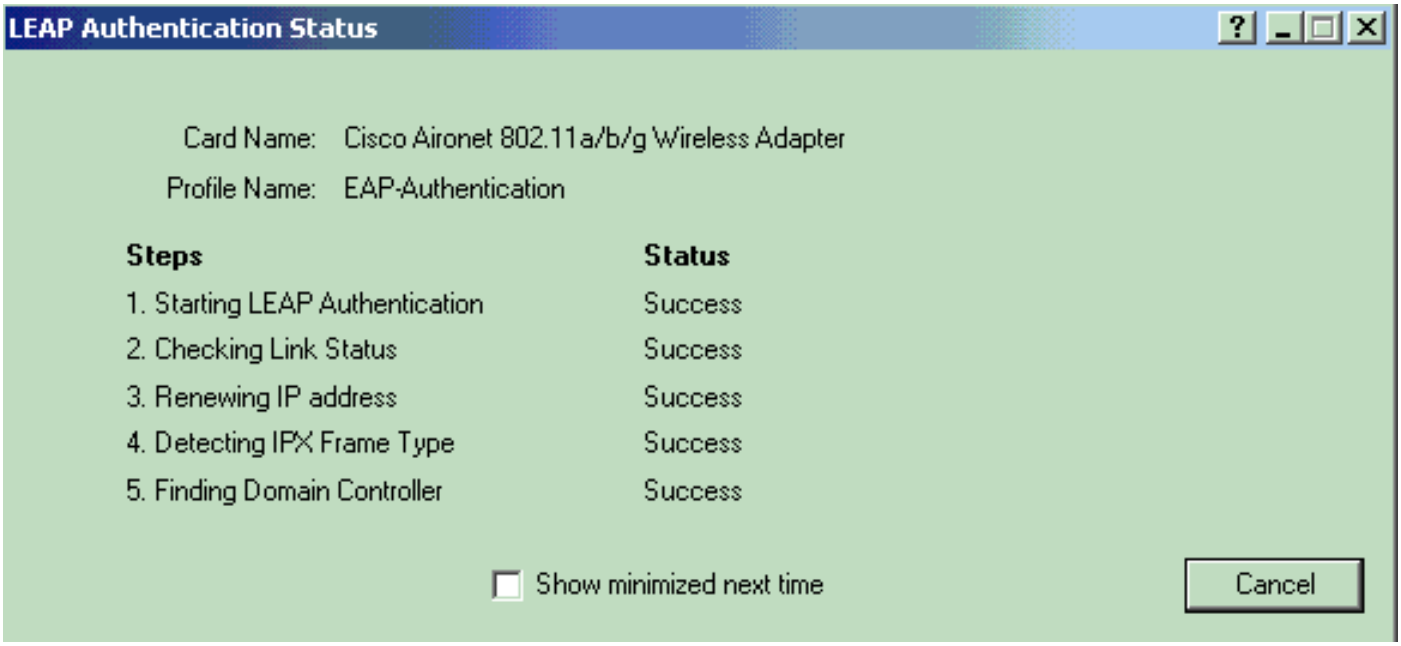
Recorde que o convidado WLAN esteve configurado para a autenticação da Web. Quando o cliente Wireless do convidado vem acima, incorpore toda a URL no navegador da Web. A página da autenticação do web padrão estala-o acima e alerta- incorporar o nome de usuário e senha. Uma vez que o usuário convidado incorpora um nome de usuário válido/senha, o WLC autentica o usuário convidado e permite o acesso à rede (possivelmente o Internet). Este exemplo mostra o indicador da autenticação da Web que o usuário recebe e a saída em uma autenticação bem sucedida:



O WLAN interno neste exemplo é configurado para a autenticação do 802.1x. Quando o cliente de WLAN interno vem acima, o cliente usa a autenticação de EAP. Para obter mais informações sobre de como configurar o cliente para a autenticação de EAP, refira a seção de utilização da autenticação de EAP do Guia de Instalação e Configuração dos adaptadores cliente do Wireless

LAN do Cisco Aironet 802.11a/b/g (CB21AG e PI21AG). Após a autenticação bem sucedida, o usuário pode alcançar a rede interna. Este exemplo mostra um cliente Wireless interno que use a autenticação do protocolo lightweight extensible authentication (PULO):





Troubleshooting

Procedimento de Troubleshooting

Use esta seção para resolver problemas de configuração.

Se a configuração não trabalha como esperado, termine estas etapas:

1. Assegure-se de que todos os VLAN configurados no WLC estejam permitidos na porta de

switch conectada ao WLC.
2. Assegure-se de que essa porta de switch que conecta ao WLC e ao roteador é configurado como uma porta de tronco.
3. Assegure-se de que os Ids VLAN usados sejam os mesmos no WLC e no roteador.
4. Verifique se os clientes recebem endereços de DHCP do servidor DHCP. Se não, verifique se o servidor DHCP é configurado corretamente. Para obter mais informações sobre dos problemas de cliente do Troubleshooting, refira pesquisando defeitos problemas de cliente na rede de Cisco Unified Wireless.

Uma das edições frequentes que ocorre com autenticação da Web é quando a reorientação à página da autenticação da Web não trabalha. O usuário não vê o indicador da autenticação da Web quando o navegador é aberto. Em lugar de, o usuário deve manualmente entrar em **https://1.1.1.1/login.html** a fim obter ao indicador da autenticação da Web. Isto tem que fazer com a pesquisa de DNS, que as necessidades de trabalhar antes da reorientação à página da autenticação da Web ocorrem. Se o homepage do navegador no cliente Wireless aponta a um Domain Name, você precisa de executar com sucesso o nslookup uma vez que o cliente associa para que a reorientação trabalhe.

Também, para um WLC que execute uma versão mais cedo do que 3.2.150.10, a maneira que os trabalhos da autenticação da Web são quando um usuário nesse SSID tenta alcançar o Internet, a interface de gerenciamento do controlador faz uma pergunta DNS para considerar se a URL é válida. Se é válida, a URL mostra a página da autorização com o endereço IP de Um ou Mais Servidores Cisco ICM NT das interfaces virtuais. Depois que o usuário inicia sessão com êxito, a solicitação original recebe permissão para retornar ao cliente. Isto é devido à identificação de bug Cisco CSCsc68105 (clientes registrados somente). Para mais informação, refira pesquisando defeitos a autenticação da Web em um controlador do Wireless LAN (WLC).

Comandos para Troubleshooting

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

Você pode usar estes comandos debug a fim pesquisar defeitos a configuração:

- **debugar o <client-MAC-endereço xx do ADDR do Mac: xx: xx: xx: xx: xx>** — Configura a eliminação de erros do MAC address para o cliente.
- **debugar o aaa que todos permitem** — Configures debuga de todos os mensagens AAA.
- **debugar o estado PEM permitem** — Configures debuga da máquina de estado do gerente da política.
- **debugar eventos PEM permitem** — Configures debuga de eventos do gerente da política.
- **debugar o mensagem DHCP permitem** — Use este comando a fim indicar a informação sobre debugging sobre as atividades DHCP Client e monitorar o estado dos pacotes DHCP.
- **debugar o pacote DHCP permitem** — Use este comando a fim indicar a informação nivelada do pacote DHCP.
- **debugar pm SSH-appgw permitem** — Configures debuga dos gateway de aplicativo.
- **debugar pm SSH-TCP permitem** — Configures debuga da manipulação tcp do gerente da política.

Estão aqui os exemplos de saída de alguns destes **comandos debug**:

Nota: Algumas linhas de saída foram envolvidas a uma segunda linha devido às razões espaciais.

(Cisco Controller) >debug dhcp message enable Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: **requested ip = 10.0.0.1** Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: vendor class id = MSFT5.0 (len 8) Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 Forwarding DHCP packet (332 octets)from 00:40:96:ac:e6:57 -- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64

(Cisco Controller) >debug dhcp packet enable Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1, encap: 0xec03 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request, client: 00:40:96:ac:e6:57: dhcp op: 1, port: 2, encap 0xec03, old mscb port number: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57 dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50, dhcpRelay: 10.0.0.10 VLAN: 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57 Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50, VLAN: 30, port: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREQUEST, htype: Ethernet,hlen: 6, hops: 1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 10.0.0.10 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50, len 350,switchport 2, vlan 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 2, encap: 0xec00 Fri Mar 2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57, frame len412, switchport 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP ACK msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 10.0.0.1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1 rcvd server id: 10.0.0.50

(Cisco Controller) >debug aaa all enable Fri Mar 2 16:22:40 2007: **User user1 authenticated** Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 **Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57** Fri Mar 2 16:22:40 2007: AuthorizationResponse: 0xbadff97c Fri Mar 2 16:22:40 2007: structureSize.....70 Fri Mar 2 16:22:40 2007: resultCode.....0 Fri Mar 2 16:22:40 2007: protocolUsed.....0x00000008 Fri Mar 2 16:22:40 2007: proxyState.....00:40:96:AC:E6:57-00:00 Fri Mar 2 16:22:40 2007: Packet contains 2 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] Service-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Unable to apply override policy for station 00:40:96:ac:e6:57 - VapAllowRadiusOverride is FALSE Fri Mar 2 16:22:40 2007: AccountingMessage Accounting Start: 0xa62700c Fri Mar 2 16:22:40 2007: Packet contains 13 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[05] Airespace /

WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:22:40 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:22:40 2007: AVP[11] Acct-Status-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[12] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:22:40 2007: AVP[13] Called-Station-Id.....10.77.244.210 (13 bytes) when web authentication is closed by user: (Cisco Controller) >Fri Mar 2 16:25:47 2007: AccountingMessage Accounting Stop: 0xa627c78 Fri Mar 2 16:25:47 2007: Packet contains 20 AVPs: Fri Mar 2 16:25:47 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:25:47 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:25:47 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:25:47 2007: AVP[11] Acct-Status-Type.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[12] Acct-Input-Octets.....0x0001820e (98830) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[13] Acct-Output-Octets.....0x00005206 (20998) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[14] Acct-Input-Packets.....0x000006ee (1774) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[15] Acct-Output-Packets.....0x00000041 (65) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[16] Acct-Terminate-Cause.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[17] Acct-Session-Time.....0x000000bb (187) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[18] Acct-Delay-Time.....0x00000000 (0) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[19] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:25:47 2007: AVP[20] Called-Station-Id.....10.77.244.210 (13 bytes)
(Cisco Controller) >debug pem state enable Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **WEBAUTH_REQD (8) Change state to START (0)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **AUTHCHECK (2) Change stateto L2AUTHCOMPLETE (4)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_NOL3SEC (14) Change state to RUN (20) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1 DHCP_REQD (7) Change stateto RUN (20) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2 DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)
(Cisco Controller) >debug pem events enable Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policy Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Replacing Fast Path rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Deleting mobile policy rule 27 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web RuleID 28 for mobile

```
00:40:96:ac:e6:57 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding
TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) ReplacingFast Path
rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo
Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57
10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007:
00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry. Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57
10.0.0.1 Added NPU entry of type 8 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU
entry of type 8
```

Informações Relacionadas

- Perguntas frequentes sobre acesso de convidado sem fio
- Exemplo de Configuração de Acesso Convidado com Fio usando Cisco WLAN Controllers
- Autenticação no exemplo de configuração dos controladores do Wireless LAN
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems