

# Exemplo de Configuração de Acesso Convidado com Fio usando Cisco WLAN Controllers

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração do switch da camada de acesso](#)

[Pontos importantes para a implantação de convidado com fio](#)

[Suporte à plataforma](#)

[Configuração de LAN sem fio](#)

[Acesso para convidado com fio e controlador de WLAN de âncora](#)

[Configuração de cliente convidado com fio](#)

[Depurações para conexão de convidado com fio em WLC local](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como configurar o acesso para convidado com o suporte ao novo recurso do acesso para convidado com fio nos controladores de WLAN da Cisco (WLCs) que usam o Software Unified Wireless da Cisco versão 4.2.61.0 e posterior. Um número cada vez maior de empresas reconhece a necessidade de fornecer acesso à Internet para clientes, parceiros e consultores, durante o acesso às suas instalações. Os gerentes de TI podem fornecer acesso seguro e controlado à Internet, com e sem fio, para convidados no mesmo controlador de LAN sem fio.

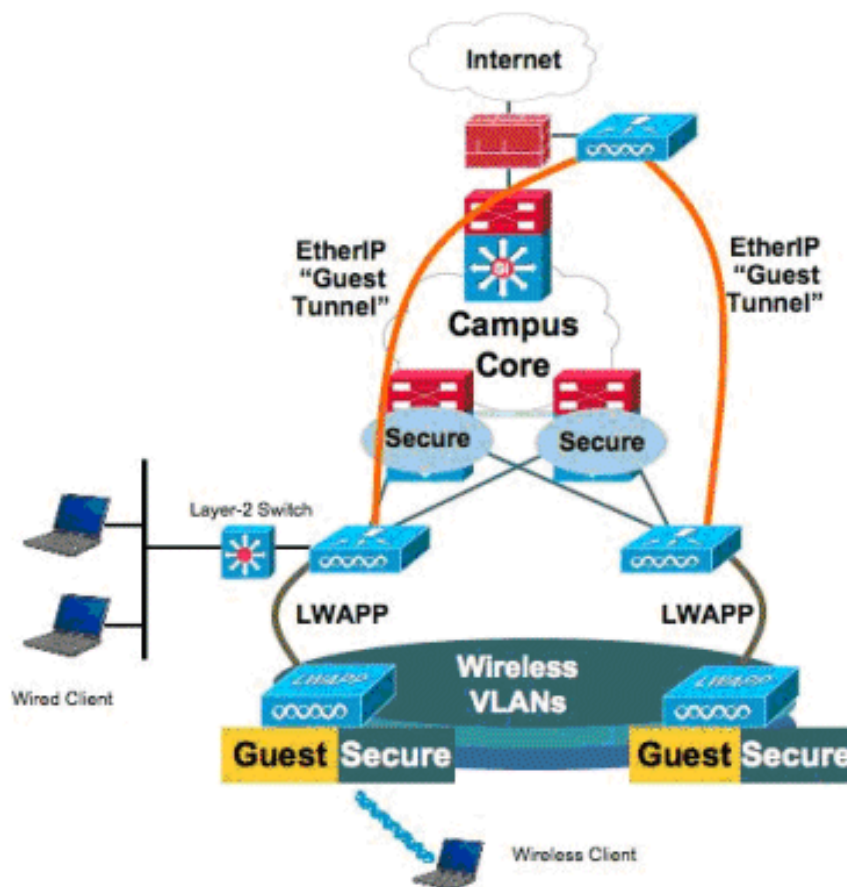
Os usuários convidados devem ter permissão para se conectar a portas Ethernet designadas e acessar a rede do convidado, conforme configurado pelo administrador, depois de concluírem os métodos de autenticação configurados. Os usuários convidados sem fio podem se conectar facilmente aos controladores de WLAN com os recursos atuais de acesso para convidado. Além disso, o Wireless Control System(WCS), juntamente com a configuração básica e o gerenciamento de controladores de WLAN, fornece serviços aprimorados de usuário convidado. Para clientes que já implantaram ou planejam implantar os controladores de WLAN e WCS na respectiva rede, podem aproveitar a mesma infraestrutura de acesso para convidado com fio. Isso fornece uma experiência de acesso unificado para convidado com e sem fio aos usuários finais.

Portas de convidado com fio são fornecidas em um local designado e conectadas a um switch de acesso. A configuração no switch de acesso coloca essas portas em uma das VLANs do convidado com fio na camada 2. Duas soluções separadas estão disponíveis para os clientes:

- Um único controlador de WLAN (modo de conversão de VLAN) - o switch de acesso

transmite o tráfego de convidado com fio na VLAN do convidado para o controlador de WLAN que fornece a solução de acesso para convidado com fio. Esse controlador realiza a conversão da VLAN de ingresso do convidado com fio até a VLAN de saída.

- Dois controladores de WLAN (modo automático de âncora) - o interruptor de acesso direciona o tráfego do convidado com fio para um controlador de WLAN local (o controlador mais próximo do switch de acesso). Esse controlador de WLAN local ancora o cliente em um controlador de WLAN de âncora de zona desmilitarizada (DMZ) configurado como acesso para convidado com e sem fio. Após uma entrega bem-sucedida do cliente ao controlador de âncora de DMZ, a atribuição de endereço IP de DHCP, a autenticação do cliente, e assim por diante, são tratadas no WLC da DMZ. Depois que ele conclui a autenticação, o cliente tem permissão para enviar/receber tráfego.



## Prerequisites

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

O suporte ao recurso de acesso para convidado com fio nos controladores de WLAN da Cisco é possibilitado pelo Software Unified Wireless da Cisco, versão 4.2.61.0 e posterior.

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.

## Configurar

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

### Configuração do switch da camada de acesso

Para oferecer o acesso para convidado com fio, as portas designadas no switch da camada de acesso 2 precisam ser configuradas pelo administrador na VLAN de convidado. A VLAN de convidado deve ser separado de quaisquer outras VLANs configuradas no switch. O tráfego de VLAN de convidado é direcionado para o controlador de WLAN local mais próximo. O controlador de local tuneliza o tráfego de convidado em uma Ethernet sobre IP (EoIP) para um controlador de âncora de DMZ. Essa solução requer pelo menos dois controladores.

Como alternativa, o switch de acesso direciona a VLAN de convidado para o controlador único e converte-a em uma interface de saída do controlador de WLAN.

```
cat6506# show vlan id 49
```

VLAN Name	Status	Ports
49 VLAN0049	active	Gi2/1, Gi2/2, Gi2/4, Gi2/35 Gi2/39, Fa4/24

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
49 enet	100049	1500	-	-	-	-	-	0	0

```
Remote SPAN VLAN
```

```
-----  
Disabled
```

Primary	Secondary	Type	Ports
---------	-----------	------	-------

```
-----
```

```
cat6506#  
interface FastEthernet4/24  
  description Wired Guest Access  
  switchport  
  switchport access vlan 49  
  no ip address  
end  
cat6506#  
interface GigabitEthernet2/4  
  description Trunk port to the WLC  
  switchport  
  switchport trunk native vlan 80  
  switchport trunk allowed vlan 49,80,110  
  switchport mode trunk  
  no ip address  
end
```

**Nota:** Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

## Pontos importantes para a implantação de convidado com fio

- Atualmente, cinco LANs de acesso para convidado com fio são aceitas. No total, 16 WLANs de usuários sem fio e 5 WLANs de acesso para convidado com fio podem ser configuradas no WLC de âncora. Não há túneis separados para WLANs. Todas as WLANs de convidado, que incluem as WLANs de acesso para convidado com fio, usam os mesmos túneis EoIP para a WLC da âncora.
- Os administradores precisam criar interfaces dinâmicas no controlador de WLAN, marcá-las como "LAN de convidado" e associá-las às WLANs criadas como LANs de convidado.
- Certifique-se de que as configurações de WLAN, incluindo a autenticação, sejam idênticas nos controladores de âncora e remotos para transmitir o tráfego do cliente.
- Os WLCs devem ter versões de software compatíveis. Certifique-se de que eles executem a mesma versão principal.
- A autenticação da Web é o mecanismo de segurança padrão disponível em uma LAN de convidado com fio. As opções atuais disponíveis são: Open, Web Auth e Web Passthrough.
- Em caso de falha do túnel EoIP, entre o computador remoto e o WLC de âncora, o banco de dados do cliente é removido do WLC de âncora. O cliente deve associar e autenticar novamente.
- Nenhuma segurança de camada 2 é aceita.
- O tráfego de multicast/transmissão nas LANs do convidado com fio é descartado.
- As configurações de proxy de DHCP devem ser idênticas às dos controladores de âncora e remotos.

Para o convidado com fio, há um limite de tempo ocioso executado no controlador. Se não forem recebidos pacotes dentro do período configurado do cliente, o cliente será removido do controlador. Da próxima vez que um cliente enviar uma solicitação de protocolo de resolução de endereço (ARP), uma nova entrada de cliente é criada e transferida para o estado de Web Auth/executar adequadamente, de acordo com a configuração de segurança.

## Suporte à plataforma

O acesso para convidado com fio é compatível com as seguintes plataformas:

- Cisco WLC 4402, 4404, WiSM, 3750g, 5508, WiSM2, WLC Virtual

## Configuração de LAN sem fio

Neste exemplo, presume-se a configuração básica do controlador de LAN sem fio. O foco é na configuração adicional necessária para concluir a implementação de acesso para convidado com fio.

1. Crie uma interface dinâmica e marque-a como "LAN de convidado". Quando você cria essa interface dinâmica na versão atual, precisa fornecer um endereço IP e gateway padrão, mesmo que ainda não exista, já que é uma VLAN de Camada 2; você não precisa fornecer nenhum endereço DHCP. Clientes convidados com fio estão fisicamente conectados a essa VLAN.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

General  
Inventory  
Interfaces  
Multicast  
Network Routes  
Internal DHCP Server  
▶ Mobility Management  
Ports  
NTP  
▶ CDP  
▶ Advanced

Interfaces > Edit

**General Information**

Interface Name	wired-vlan-49
MAC Address	00:18:b9:ea:a7:23

**Interface Address**

VLAN Identifier	49
IP Address	10.10.49.2
Netmask	255.255.255.0
Gateway	10.10.49.1

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

**Configuration**

Quarantine	<input type="checkbox"/>
Guest Lan	<input checked="" type="checkbox"/>

**DHCP Information**

Primary DHCP Server	
Secondary DHCP Server	

**Access Control List**

ACL Name	none
----------	------

*Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.*

2. Crie outra interface dinâmica para que os clientes convidados com fio recebam um endereço IP. **Note:** Você precisa fornecer um endereço IP/gateway padrão/endereço de servidor de DHCP nessa interface.

**Controller**

- General
- Inventory
- Interfaces
- Multicast
- Network Routes
- Internal DHCP Server
- ▶ Mobility Management
- Ports
- NTP
- ▶ CDP
- ▶ Advanced

**Interfaces > Edit**

**General Information**

Interface Name: 110  
 MAC Address: 00:18:b9:ea:a7:23

**Interface Address**

VLAN Identifier: 110  
 IP Address: 10.10.110.2  
 Netmask: 255.255.255.0  
 Gateway: 10.10.110.1

**Physical Information**

Port Number: 1  
 Backup Port: 0  
 Active Port: 1  
 Enable Dynamic AP Management:

**Configuration**

Quarantine:   
 Guest Lan:

**DHCP Information**

Primary DHCP Server: 10.10.110.1  
 Secondary DHCP Server:

**Access Control List**

ACL Name: none

*Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.*

3. Estas são as interfaces dinâmicas:

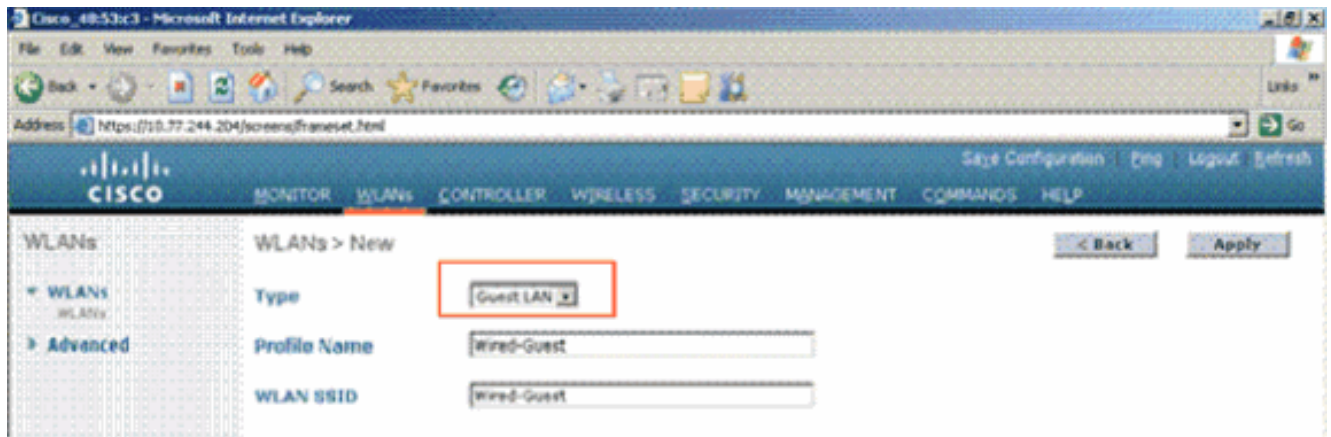
**Controller**

- General
- Inventory
- Interfaces
- Multicast
- Network Routes
- Internal DHCP Server
- ▶ Mobility Management
- Ports

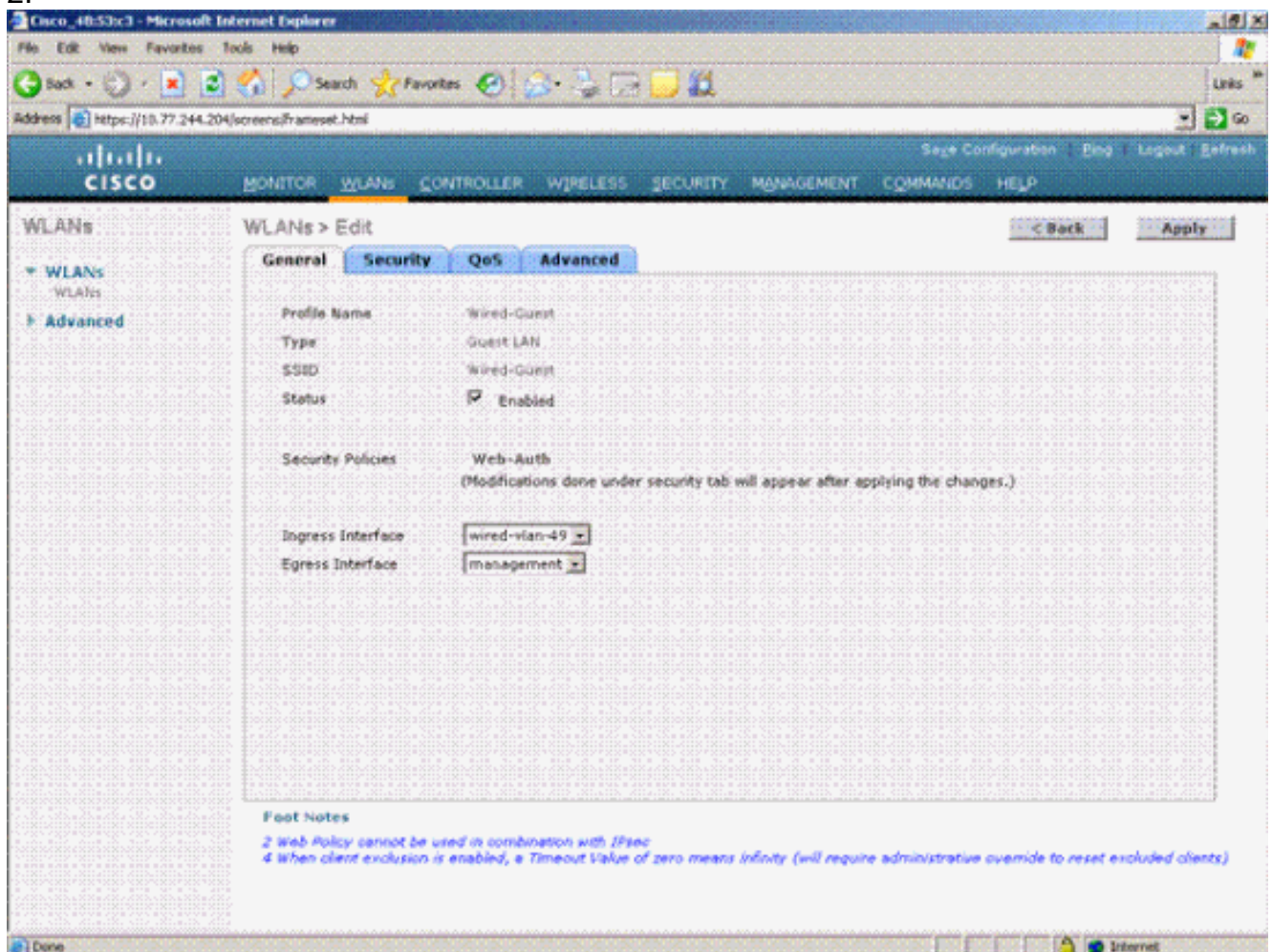
**Interfaces**

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
<a href="#">110</a>	110	10.10.110.2	Dynamic	Disabled
<a href="#">ap-manager</a>	untagged	10.10.80.4	Static	Enabled
<a href="#">management</a>	untagged	10.10.80.3	Static	Not Supported
<a href="#">service-port</a>	N/A	0.0.0.0	Static	Not Supported
<a href="#">virtual</a>	N/A	1.1.1.1	Static	Not Supported
<a href="#">wired-vlan-49</a>	49	10.10.49.2	Dynamic	Disabled

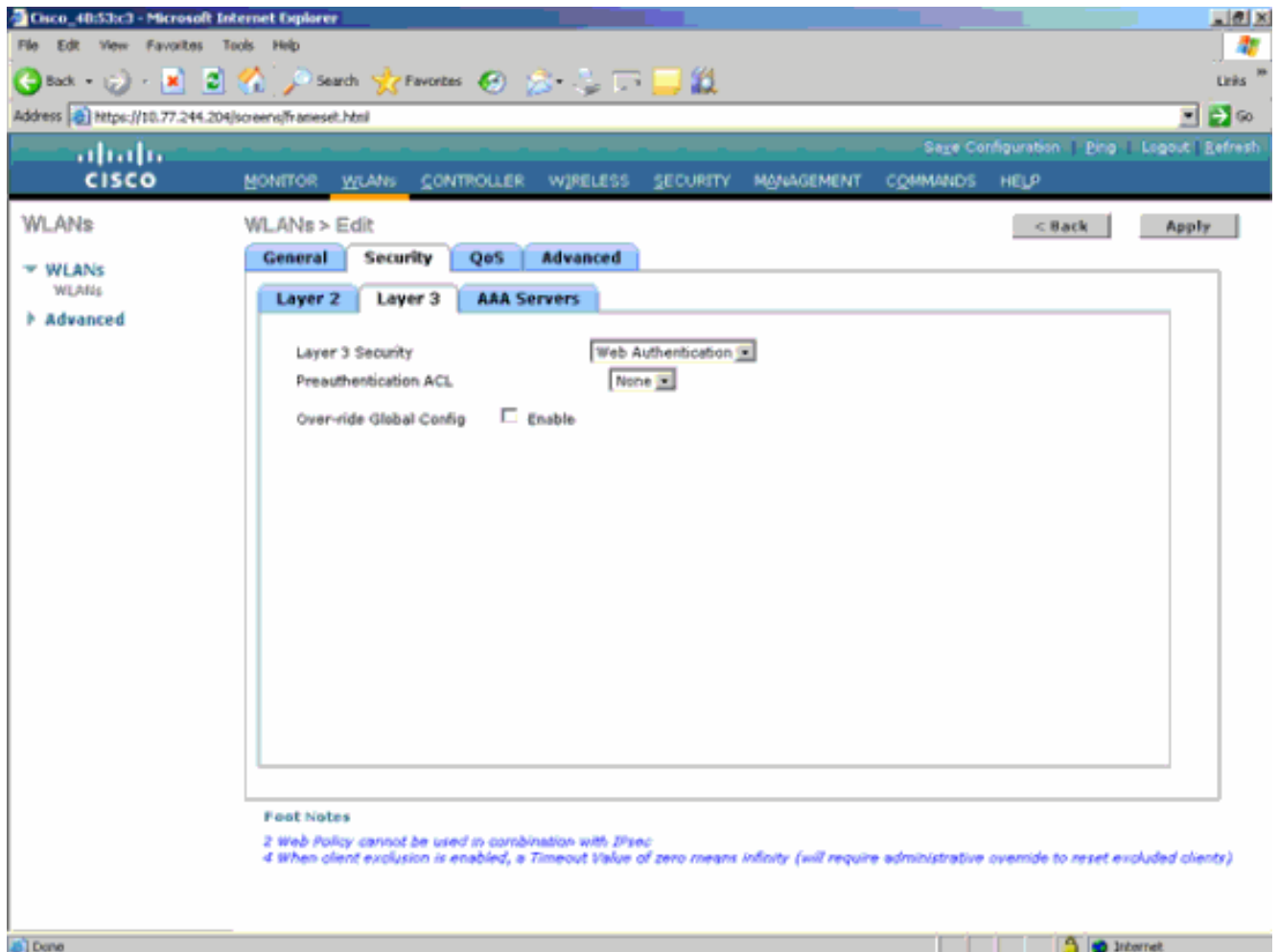
4. Adicionar uma nova WLAN: Tipo = LAN de convidado.



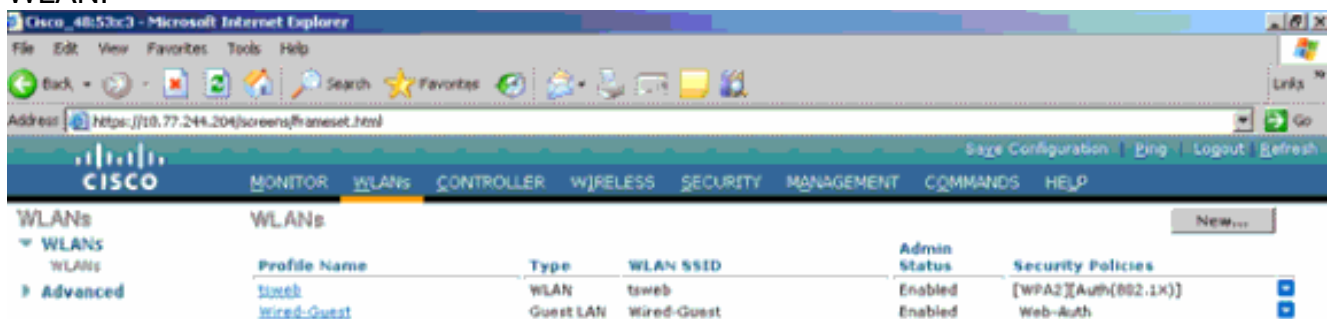
5. Ativar a WLAN; mapeie a interface de ingresso para a "LAN de convidado" criada na Etapa 1, e a interface de saída pode ser uma interface de gerenciamento ou qualquer outra interface dinâmica, embora de preferência uma interface dinâmica como a criada na Etapa 2.



6. A autenticação da Web está ativada por padrão como a opção de segurança configurada na LAN de convidado. Ela pode ser alterada para *Nenhuma* ou *Web Passthrough*

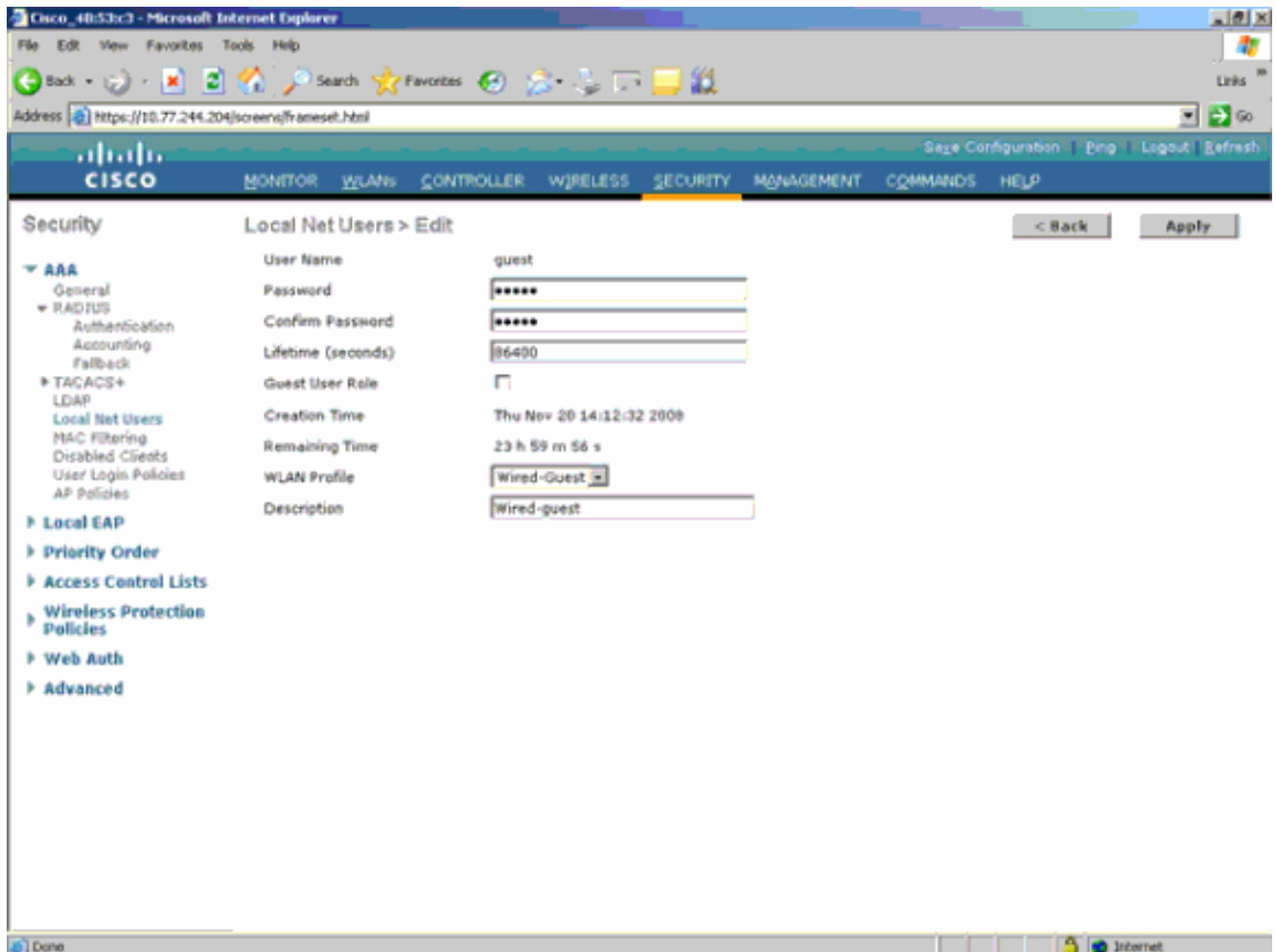


7. Essa é a configuração final da WLAN.



8. Adicione um usuário convidado no banco de dados local do WLC.





No Exterior, você precisa definir a entrada como a "LAN de convidado" configurada. Na saída, é necessário defini-la como uma interface, possivelmente a interface de gerenciamento. No entanto, depois que o túnel EoIP foi criado, ela envia o tráfego automaticamente pelo túnel em vez do endereço de gerenciamento.

## Acesso para convidado com fio e controlador de WLAN de âncora

Neste exemplo, o endereço IP do controlador de LAN sem fio remoto é 10.10.80.3 e o endereço IP do controlador de âncora de DMZ é 10.10.75.2. Ambos são parte de dois grupos diferentes de mobilidade.

1. Configure o grupo de mobilidade do controlador de âncora de DMZ quando você adiciona o endereço MAC, o endereço IP e o nome de grupo de mobilidade do controlador remoto.

The screenshot shows the Cisco Controller GUI with the 'CONTROLLER' tab selected. The left sidebar contains a navigation menu with 'Mobility Management' expanded to 'Mobility Groups'. The main content area is titled 'Mobility Group Members > Edit All'. It includes a descriptive paragraph and a text area containing the following text:

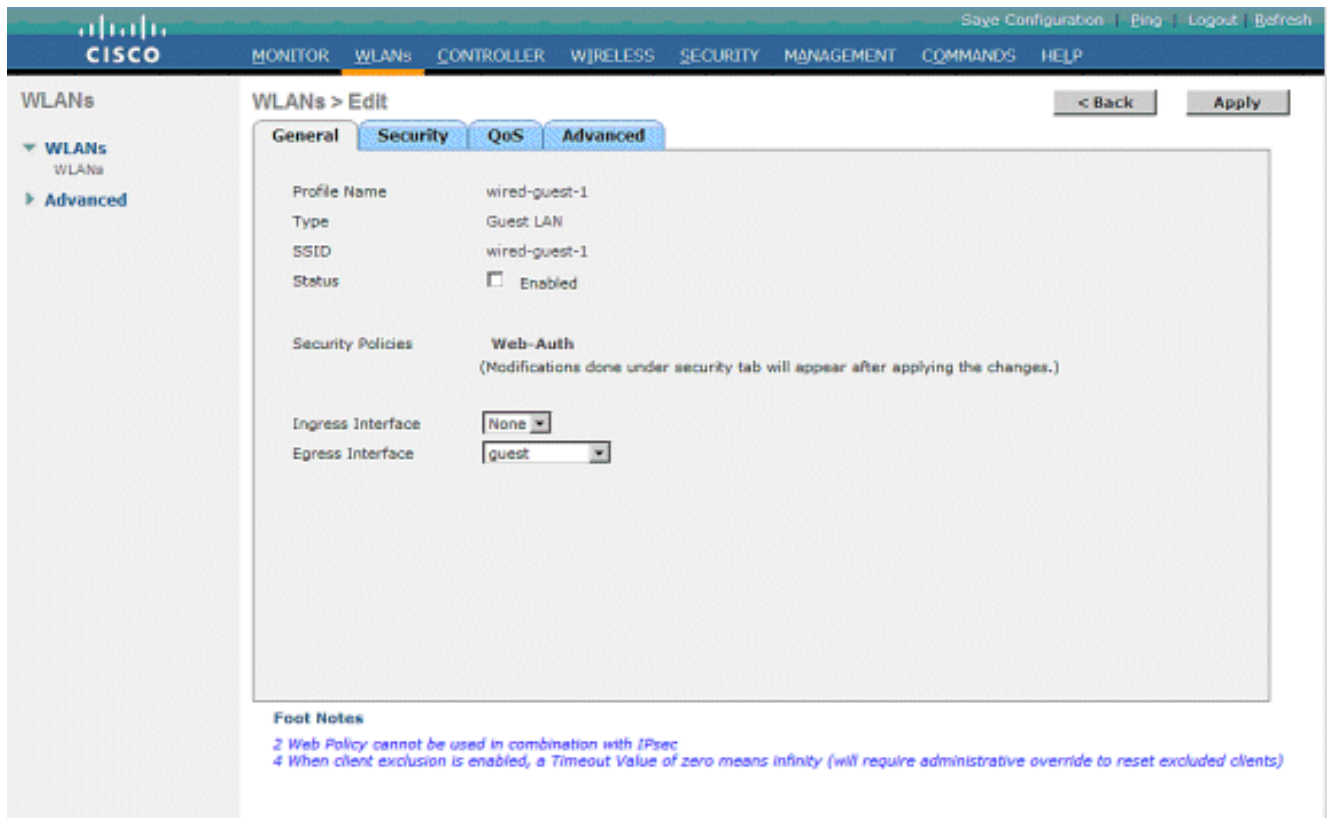
```
00:18:73:34:b2:60 10.10.75.2
00:18:b9:ea:a7:20 10.10.80.3 mobile-10
```

2. Da mesma forma, configure o grupo de mobilidade no controlador remoto.

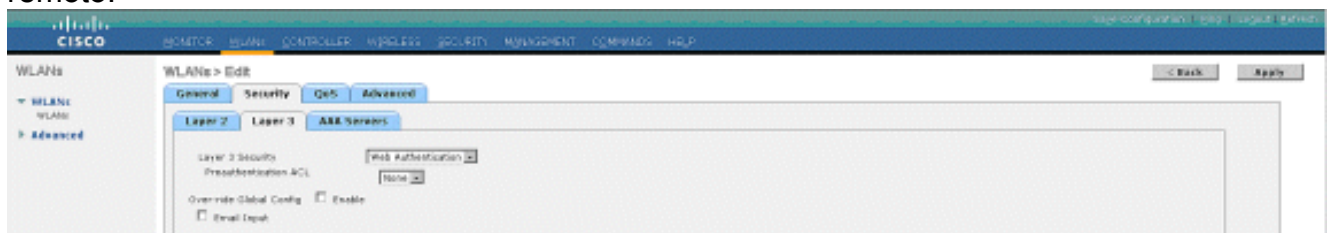
This screenshot is similar to the first one, but the text area in the 'Mobility Group Members > Edit All' section contains the following text:

```
00:18:b9:ea:a7:20 10.10.80.3
00:18:73:34:b2:60 10.10.75.2 mobile-9
```

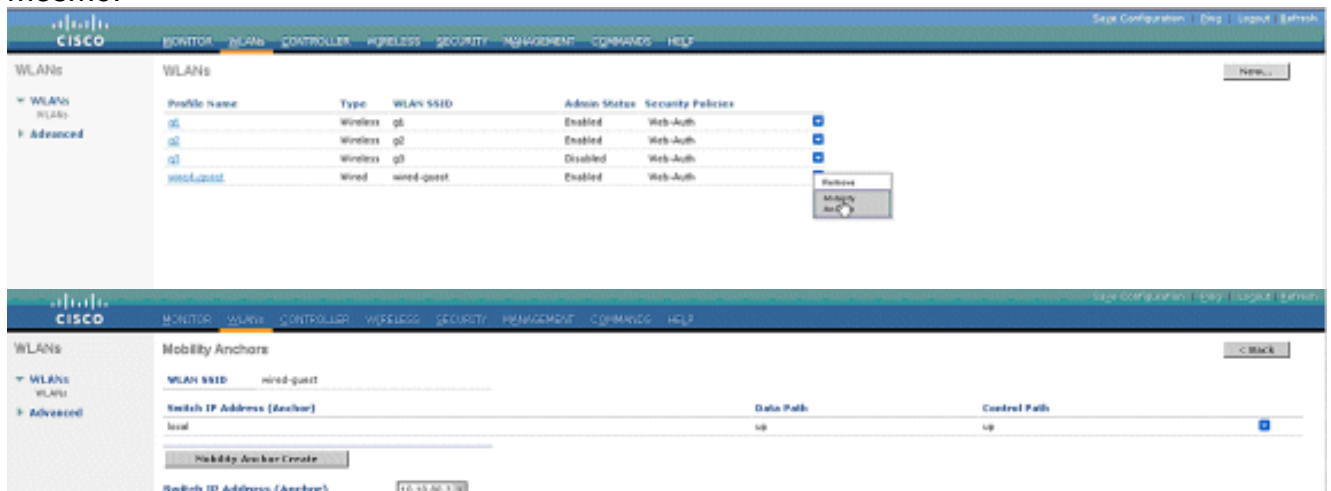
3. Crie a WLAN com fio usando o nome exato no WLC de âncora. A interface de ingresso nesse caso é "none" porque, logicamente, a interface de ingresso é o túnel EoIP do controlador remoto. A interface de saída é uma interface diferente, onde os clientes com fio recebem o endereço IP. Neste exemplo, uma interface dinâmica chamada *convidado* é criada. No entanto, você não pode ativar a WLAN nessa fase porque ela exibe a mensagem de erro de que uma interface de ingresso não pode ser *nenhuma*.



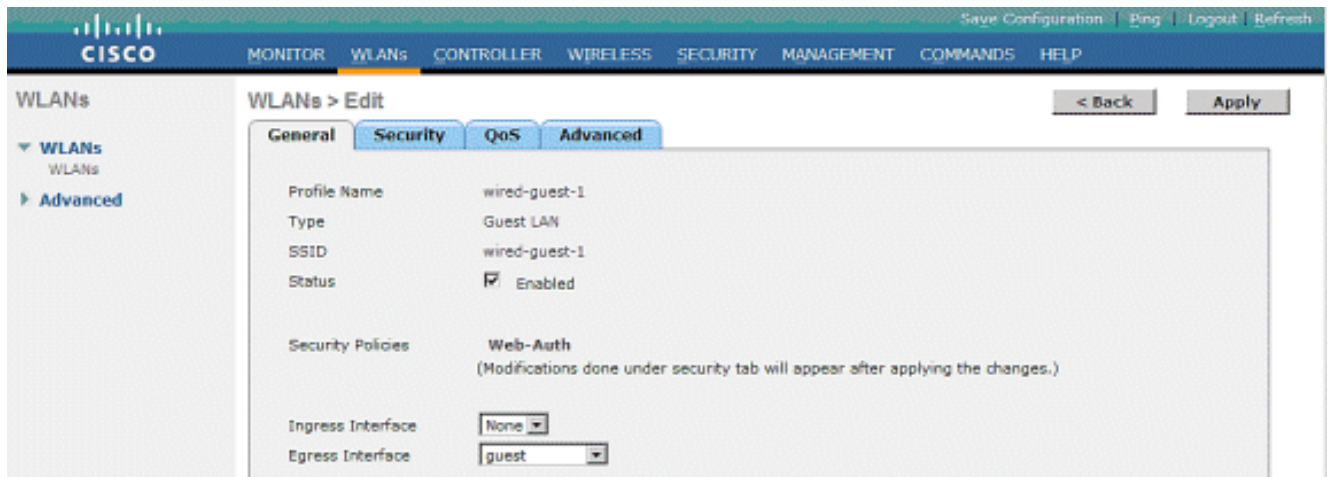
4. Configure a segurança de camada 3 como *autenticação da web*, semelhante ao controlador remoto.



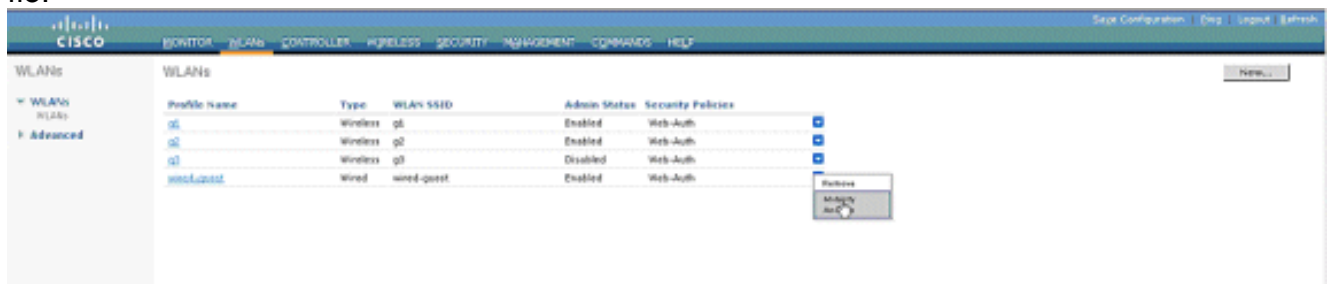
5. Crie a âncora de mobilidade no controlador de âncora e mapeie para ele mesmo.



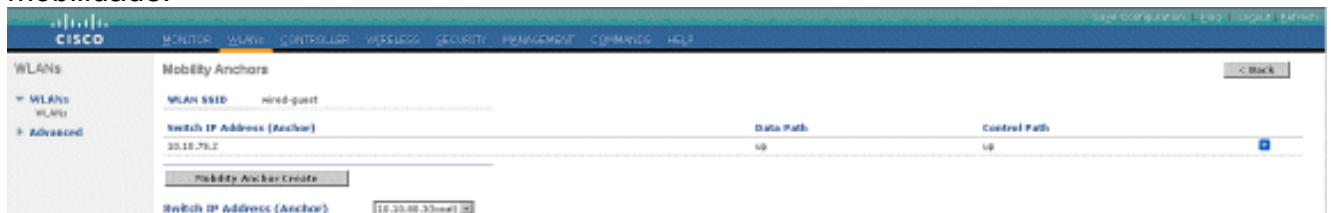
6. Depois que a âncora de mobilidade for criada, volte e ative a WLAN com fio.



7. Da mesma forma, crie a âncora de mobilidade no WLC remoto para a WLAN de convidado com fio.



Escolha o endereço IP do WLC da âncora e, também, a âncora de mobilidade.



Verifique se o caminho de dados e de controle está ativo. Caso contrário, certifique-se de que essas portas estejam abertas entre o controlador de LAN sem fio de âncora e remoto: UDP 16666 ou IP 97.

8. Quando um usuário convidado com fio estiver conectado ao switch e tiver concluído a autenticação da Web, o Policy Manager State (Estado do gerenciador de políticas) deverá ser RUN (EXECUTAR) e Mobility Role (Função de Mobilidade) será Export Foreign (Exportar externo).

The screenshot shows the Cisco WLC interface with the 'Clients > Detail' page. The 'Client Properties' table is as follows:

Client Properties	
MAC Address	00:0d:60:5e:ca:62
IP Address	0.0.0.0
Client Type	Regular
User Name	
Port Number	1
Interface	110
VLAN ID	110
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Export Foreign
Mobility Peer IP Address	10.10.75.2
Policy Manager State	RUN
Mirror Mode	Disable
Management Frame Protection	No

The 'AP Properties' table is as follows:

AP Properties	
AP Address	Unknown
AP Name	N/A
AP Type	Unknown
WLAN Profile	wired-guest-1
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0

Da mesma forma, verifique o status no WLC de âncora. O Policy Manager State (Estado do gerenciador de políticas) deverá ser RUN (EXECUTAR) e Mobility Role (Função de Mobilidade) será Export Anchor (Exportar âncora).

The screenshot shows the Cisco WLC interface with the 'Clients > Detail' page. The 'Client Properties' table is as follows:

Client Properties	
MAC Address	00:0d:60:5e:ca:62
IP Address	10.10.77.11
Client Type	Regular
User Name	guest
Port Number	1
Interface	guest
VLAN ID	77
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Export Anchor
Mobility Peer IP Address	10.10.80.3
Policy Manager State	RUN
Mirror Mode	Disable
Management Frame Protection	No

The 'AP Properties' table is as follows:

AP Properties	
AP Address	Unknown
AP Name	10.10.80.3
AP Type	Mobile
WLAN Profile	wired-guest-1
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0

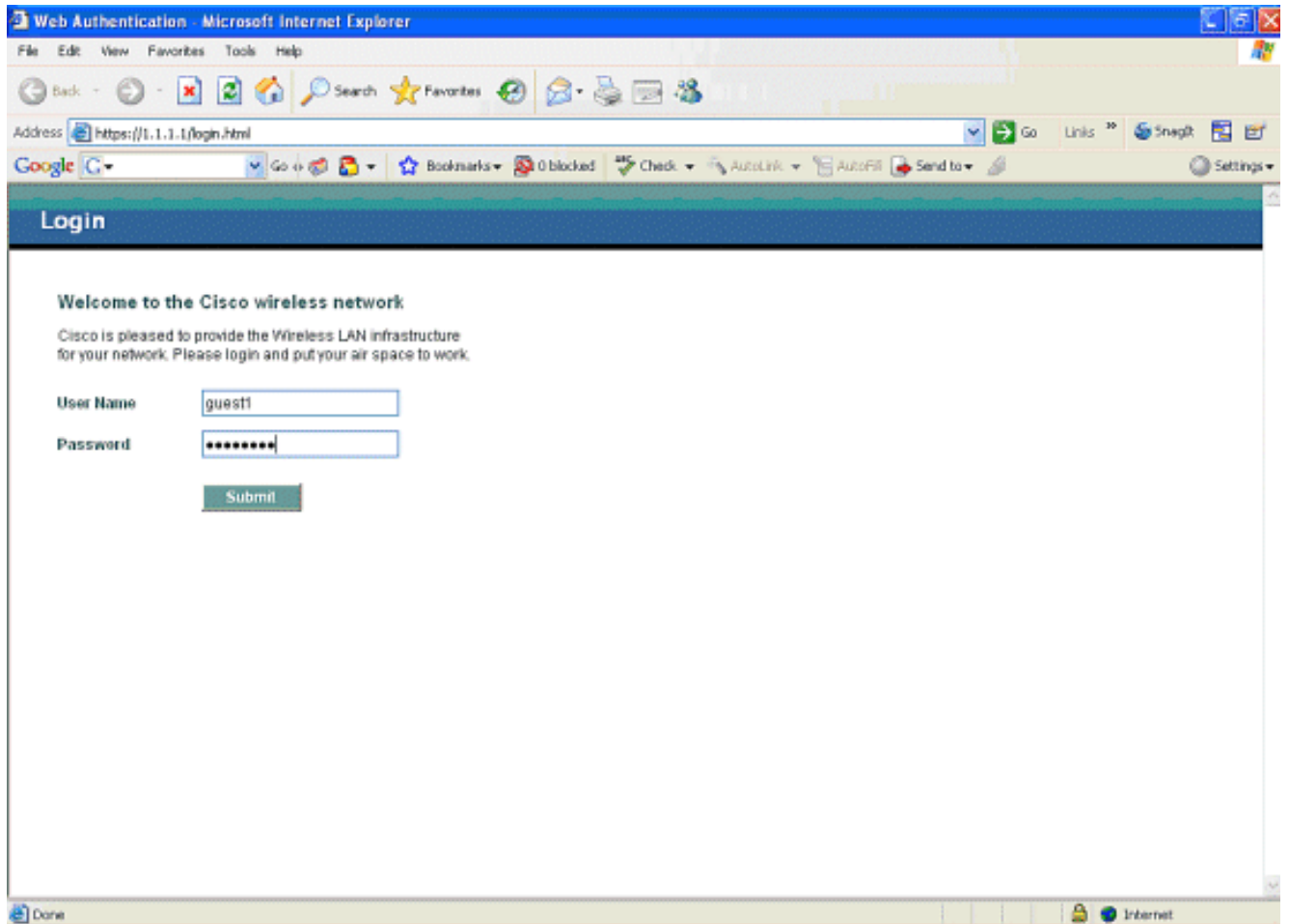
## Configuração de cliente convidado com fio

O cliente convidado com fio recebe um endereço IP da VLAN de saída, mas não pode transmitir nenhuma tráfego até a conclusão do processo de autenticação da Web.

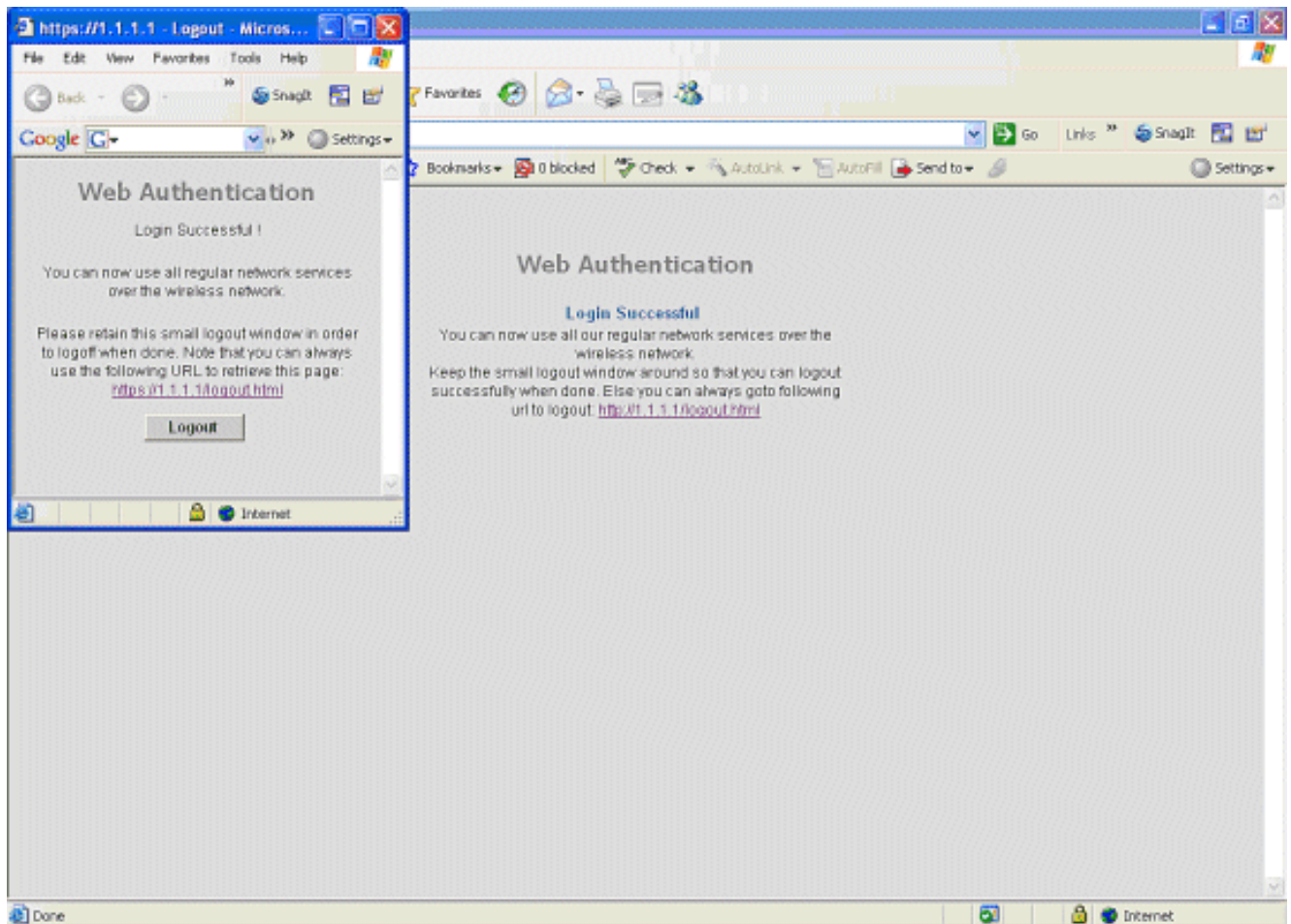
Para fazer logon como um usuário convidado, siga estas etapas:

1. Abra uma janela do navegador e digite o nome do URL desejado (por exemplo, [www.cisco.com](http://www.cisco.com)). O convidado será redirecionado para a página da Web padrão do controlador de LAN sem fio se a autenticação da Web estiver ativada e uma resolução DNS puder ser concluída para o URL inserido. Caso contrário, insira este URL: <https://1.1.1.1/login.html>, em que o endereço IP 1.1.1.1 é o endereço IP virtual do

controlador de LAN sem fio.



2. Insira o nome de usuário e a senha fornecidos.
3. Se o logon for bem-sucedido, uma janela do navegador avisa isso.



## Depurações para conexão de convidado com fio em WLC local

Essa depuração fornece todas as informações relacionadas ao cliente convidado com fio.

### debug client

```

Cisco Controller) >show debug
MAC address ..... 00:0d:60:5e:ca:62
Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.

(Cisco Controller) >Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  Adding mobile on Wired Guest 00:00:00:00:00:00(0)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  apfHandleWiredGuestMobileStation
  (apf_wired_guest.c:121) Changing state for mobile
    00:0d:60:5e:ca:62 on AP 00:00:00:
00:00:00 from Idle to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
  Initializing policy

```

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)  
Change state to AUTHCHECK (2) last state AUTHCHECK (2)  
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 AUTHCHECK (2)  
Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)  
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 L2AUTHCOMPLETE (4)  
Change state to DHCP\_REQD (7) last state DHCP\_REQD (7)  
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62  
apfPemAddUser2 (apf\_policy.c:209) Changing state for mobile  
00:0d:60:5e:ca:62 on AP 00:00:00:00:00:00 from Associated to Associated  
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 Session Timeout is 0 -  
not starting session timer for the mobile  
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62  
Stopping deletion of Mobile Station: (callerId: 48)  
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62  
**Wired Guest packet from 10.10.80.252 on mobile**  
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62  
Wired Guest packet from 10.10.80.252 on mobile  
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62  
Orphan Packet from 10.10.80.252  
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62  
Wired Guest packet from 169.254.20.157 on mobile  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62  
Wired Guest packet from 169.254.20.157 on mobile  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0  
**DHCP\_REQD (7) State Update from Mobility-Incomplete  
to Mobility-Complete, mobility role=Local**  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0  
DHCP\_REQD (7) pemAdvanceState2 3934, Adding TMP rule  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0  
DHCP\_REQD (7) Adding Fast Path rule  
type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00,  
slot 0, interface = 1, QOS = 0 ACL Id = 255,  
Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0 DHCP\_REQD  
(7) Successfully plumbed mobile rule (ACL ID 255)  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62  
Installing Orphan Pkt IP address 169.254.20.157 for station  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62  
Unsuccessfully installed IP address 169.254.20.157 for station  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62  
0.0.0.0 Added NPU entry of type 9  
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62  
Sent an XID frame  
Tue Sep 11 13:27:45 2007: 00:0d:60:5e:ca:62  
Wired Guest packet from 169.254.20.157 on mobile  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP selecting relay 1 - control block settings:  
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,  
dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
**DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,  
gateway 10.10.110.1, VLAN 110, port 1)**  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP transmitting DHCP DISCOVER (1)  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP xid: 0x87214d01 (2267106561),secs: 0, flags: 8000  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP chaddr: 00:0d:60:5e:ca:62  
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0



Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP requested ip:10.10.80.252

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP ARPing for 10.10.110.1 (SPA 10.10.110.2, vlanId 110)

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP selecting relay 2 - control block settings:  
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,  
**dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2**  
**VLAN: 110**

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62  
DHCP selected relay 2 - NONE

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP selecting relay 1 - control block settings:  
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,  
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,  
gateway 10.10.110.1, VLAN 110, port 1)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP transmitting DHCP DISCOVER (1)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP requested ip: 10.10.80.252

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP sending REQUEST to 10.10.110.1 (len 350, port 1, vlan 110)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP selecting relay 2 - control block settings:  
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,  
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62  
DHCP selected relay 2 - NONE

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP setting server from OFFER  
(server 10.10.110.1, yiaddr 10.10.110.3)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP sending REPLY to Wired Client (len 350, port 1)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP transmitting DHCP OFFER (2)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP xid: 0x87214d01 (2267106561), secs: 0, flags: 8000

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP ciaddr: 0.0.0.0, yiaddr: 10.10.110.3

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP server id: 1.1.1.1 rcvd server id: 10.10.110.1

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP received op BOOTREQUEST (1) (len 334, port 1, encap 0xec00)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP selecting relay 1 - control block settings:  
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,  
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,  
gateway 10.10.110.1, VLAN 110, port 1)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP transmitting DHCP REQUEST (3)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**DHCP requested ip: 10.10.110.3**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**DHCP server id: 10.10.110.1 rcvd server id: 1.1.1.1**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**DHCP sending REQUEST to 10.10.110.1(len 374, port 1, vlan 110)**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**DHCP selecting relay 2 - control block settings:**  
**dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,**  
**dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP selected relay 2 -NONE

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**10.10.110.3 DHCP REQD (7) Change state to WEBAUTH\_REQD**  
**(8) last state WEBAUTH\_REQD (8)**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
10.10.110.3 WEBAUTH\_REQD (8) pemAdvanceState2  
4598, Adding TMP rule

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**10.10.110.3 WEBAUTH\_REQD (8) Replacing Fast Path rule**  
**type = Airespace AP Client - ACL passthru**  
**on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0**  
**ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
**10.10.110.3 WEBAUTH\_REQD (8) Successfully**  
**plumbed mobile rule (ACL ID 255)**

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
Plumbing web-auth redirect rule due to user logout

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
Adding Web RuleID 31 for mobile 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
Assigning Address 10.10.110.3 to mobile

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP sending REPLY to Wired Client (len 350, port 1)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP transmitting DHCP ACK (5)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62  
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62

```
DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP   chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP   ciaddr: 0.0.0.0, yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP   siaddr: 0.0.0.0, giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP   server id: 1.1.1.1 rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
10.10.110.3 Added NPU entry of type 2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62 Sent an XID frame
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
Username entry (guest1) created for mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
Setting guest session timeout for mobile
00:0d:60:5e:ca:62 to 79953 seconds
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
Session Timeout is 79953 - starting session timer for the mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_REQD (8) Change state to
WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_NOL3SEC (14) Change state to RUN
(20) last state RUN (20)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
(20) Reached PLUMBFA STPATH: from line 4518
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
(20) Replacing FastPath rule
type = Airespace AP Client
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3
Added NPU entry of type 1
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 Sending a gratuitous
ARP for 10.10.110.3, VLAN Id 110
```

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Configuração da mobilidade de âncora automática](#)
- [WLAN de convidado e WLAN interna usando o exemplo de configuração de WLCs](#)
- [Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers](#)
- [Guia de configuração de Cisco Wireless LAN Controller, versão 4.2](#)
- [Suporte de produtos Wireless](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.