

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

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

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

[Pontos importantes para o desenvolvimento prendido do convidado](#)

[Suporte à plataforma](#)

[Configuração do Wireless LAN](#)

[Acesso prendido do convidado com controlador de WLAN da âncora](#)

[Configuração de cliente prendida do convidado](#)

[Debuga para a conexão prendida do convidado no WLC local](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o acesso do convidado com o apoio prendido novo dos recursos de acesso do convidado nos controladores de WLAN de Cisco (WLC) esse Software Release 4.2.61.0 e Mais Recente do Cisco Unified Wireless do uso. Um número crescente de empresas reconhecem a necessidade de fornecer o acesso ao Internet a seus clientes, os Parceiros, e os consultantes quando visita suas facilidades. Os gerentes TI podem prever acesso fixado e controlado prendido e do Sem fio ao Internet convidados no mesmo controlador do Wireless LAN.

Os usuários convidado devem ser permitidos conectar às portas Ethernet designadas e alcançar a rede de convidado como configurados pelo administrador depois que terminam os métodos de autenticação configurados. Os usuários convidado wireless podem facilmente conectar aos controladores de WLAN com os recursos de acesso atuais do convidado. Além, o sistema de controle wireless (WCS), junto com a configuração básica e o Gerenciamento dos controladores de WLAN, proporciona serviços aumentados do usuário convidado. Para os clientes que já têm distribuído ou os planeiam distribuir controladores de WLAN e WCS em sua rede, podem leverage a mesma infraestrutura para o acesso prendido do convidado. Isto fornece uma experiência wireless e prendida unificada do acesso do convidado aos utilizadores finais.

As portas prendidas do convidado são fornecidas em um lugar designado e obstruídas em um switch de acesso. A configuração no switch de acesso põe estas portas em uma da camada

prendida 2 VLAN do convidado. Duas soluções separadas estão disponíveis aos clientes:

- Um único controlador de WLAN (modo da tradução de vlan) - os troncos do switch de acesso o tráfego prendido do convidado no convidado VLAN ao controlador de WLAN que fornece a solução de acesso prendida do convidado. Este controlador realiza a tradução de vlan do convidado prendido ingresso VLAN à saída VLAN.
- Dois controladores de WLAN (auto modo da âncora) - os troncos do switch de acesso o tráfego prendido do convidado a um controlador de WLAN local (controlador o mais próximo ao switch de acesso). Este controlador de WLAN do local ancora o cliente em um controlador de WLAN da âncora da zona desmilitarizada (DMZ) que seja configurado para o acesso prendido e wireless do convidado. Após uma entrega bem sucedida do cliente ao controlador da âncora DMZ, a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT DHCP, autenticação do cliente, é segurada e assim por diante no DMZ WLC. Depois que termina a autenticação, está permitido enviar/recebe ao cliente o tráfego.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

O apoio prendido dos recursos de acesso do convidado nos controladores de WLAN de Cisco é apoiado pelo Software Release 4.2.61.0 e Mais Recente do Cisco Unified Wireless.

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.

Configurar

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

Configuração do switch de camada de acesso

A fim fornecer o acesso prendido do convidado, as portas designadas na necessidade do switch de camada de acesso da camada 2 de ser configurado no convidado VLAN pelo administrador. O convidado VLAN deve ser separa de todos os outros VLAN que forem configurados neste interruptor. O tráfego de VLAN do convidado é em tronco ao controlador o mais próximo do local WLAN. O controlador do local escava um túnel o tráfego do convidado através de um Ethernet sobre o túnel IP (EoIP) a um controlador da âncora DMZ. Esta solução exige pelo menos dois controladores.

Alternativamente, os troncos do switch de acesso o convidado VLAN ao único controlador traduzem o convidado VLAN à 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 Transl 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 ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

Pontos importantes para o desenvolvimento prendido do convidado

- Atualmente, cinco o convidado LAN para o acesso prendido do convidado é apoiado. No total, 16 WLAN para usuários Wireless e 5 WLAN para o acesso prendido do convidado podem ser configurados na âncora WLC. Nenhum túnel separado existe para WLAN. Todo o convidado WLAN, que incluem os WLAN para o acesso prendido do convidado, usa os mesmos túneis de EoIP à âncora WLC.
- Os administradores precisam de criar interfaces dinâmica no controlador de WLAN, de marcá-las como o “convidado LAN,” e de associá-las aos WLAN criados como o convidado LAN.
- Assegure-se de que as configurações WLAN, incluindo a autenticação, estejam idênticas na âncora e em controladores remotos passar o tráfego do cliente.
- Os WLC devem ter versões de software compatíveis. Assegure-se de que executem a mesma versão principal.
- A autenticação da Web é o mecanismo de segurança do padrão disponível em um convidado

prendido LAN. As opções atuais disponíveis são estas: Abra, AUTH da Web, e transmissão da Web.

- Em caso da falha do túnel de EoIP entre o telecontrole e a âncora WLC, o base de dados do cliente é limpo da âncora WLC. O cliente precisa de reassociar e reauthenticate.
- Nenhuma Segurança da camada 2 é apoiada.
- O Multicast/tráfego de broadcast no convidado prendido LAN é deixado cair.
- Os ajustes do proxy DHCP devem ser idênticos na âncora e em controladores remotos.

Para o convidado prendido, há um idle timeout que é executado no controlador. Se nenhum pacote é recebido dentro do período configurado do cliente, o cliente está removido do controlador. Quando um cliente envia uma requisição de protocolo de resolução de endereço (ARP) a próxima vez, uma entrada de cliente nova está criada e movida para o AUTH da Web/estado de corrida apropriadamente conforme a configuração de segurança.

Suporte à plataforma

O convidado prendido alcança é apoiado nestas Plataformas:

- Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM2, WLC virtual

Configuração do Wireless LAN

Neste exemplo, a configuração básica do controlador do Wireless LAN é suposta. O foco está na configuração adicional exigida para terminar a aplicação prendida do acesso do convidado.

1. Crie uma interface dinâmica e marque-a é como um “convidado LAN.” Quando você cria esta interface dinâmica na versão atual, você precisa de fornecer um endereço IP de Um ou Mais Servidores Cisco ICM NT e um gateway padrão, mesmo que não exista desde que é uma camada 2 VLAN; você não precisa de fornecer nenhum endereço de DHCP. Os clientes prendidos do convidado são conectados fisicamente a este VLAN.
2. Crie uma outra interface dinâmica onde os clientes prendidos do convidado recebam um endereço IP de Um ou Mais Servidores Cisco ICM NT. Nota: Você precisa de fornecer um endereço IP de Um ou Mais Servidores Cisco ICM NT/endereço do servidor do gateway padrão /DHCP nesta relação.
3. Estas são as interfaces dinâmica:
4. Adicionar um WLAN novo: Type=Guest LAN.
5. Permita o WLAN; trace a interface de ingresso ao “convidado LAN” criado em etapa 1, e a interface de saída pode ser uma interface de gerenciamento ou toda a outra interface dinâmica, embora preferivelmente uma interface dinâmica tal como aquela criada em etapa 2.
6. A autenticação da Web é permitida à revelia como a opção de segurança configurada no convidado LAN. Pode ser mudada à *transmissão nenhuns* ou da *Web*.
7. Esta é a configuração final do WLAN.
8. Adicionar um usuário convidado no base de dados local do WLC. No estrangeiro, você precisa de ajustar o ingresso como o “convidado configurado LAN.” Na saída, você precisa de ajustá-la a alguma relação, possivelmente a interface de gerenciamento. Contudo, uma vez que o túnel de EoIP é construído, envia o tráfego automaticamente através do túnel em vez do endereço de gerenciamento.

O convidado prendido alcança com controlador de WLAN da âncora

Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador remoto do Wireless LAN é 10.10.80.3, e o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador da âncora DMZ é 10.10.75.2. Ambos são parte de dois Grupos de mobilidade diferentes.

1. Configurar o grupo da mobilidade do controlador da âncora DMZ quando você adiciona o MAC address, o endereço IP de Um ou Mais Servidores Cisco ICM NT, e o nome do grupo da mobilidade do controlador remoto.
2. Similarmente, configurar o grupo da mobilidade no controlador remoto.
3. Crie o WLAN prendido com o nome exato na âncora WLC. A interface de ingresso não é neste caso “nenhuma” porque, logicamente, a interface de ingresso é o túnel de EoIP do controlador remoto. A interface de saída é uma relação diferente, aonde os clientes prendidos vão receber o endereço IP de Um ou Mais Servidores Cisco ICM NT. Neste exemplo, uma interface dinâmica chamada *convidado* é criada. Contudo, nesta fase você não pode permitir o WLAN porque indica um Mensagem de Erro, que leia que uma interface de ingresso não pode ser *nenhuma*.
4. Configurar a Segurança da camada 3 como a *autenticação da Web*, similar ao controlador remoto.
5. Crie a âncora da mobilidade no controlador da âncora, e setrace-a.
6. Uma vez que a âncora da mobilidade é criada, vá para trás e permita o WLAN prendido.
7. Similarmente, crie a âncora da mobilidade no WLC remoto para o convidado prendido WLAN. Escolha o endereço IP de Um ou Mais Servidores Cisco ICM NT da âncora WLC e crie a âncora da mobilidade. Verifique se os dados e o trajeto do controle estão acima. Se não, assegure-se de que estas portas estejam abertas entre a âncora e o controlador remoto do Wireless LAN: UDP 16666 ou IP 97.
8. Uma vez que um usuário convidado prendido é conectado ao interruptor e terminou a autenticação da Web, o estado do gerente da política deve SER EXECUTADO, e o papel da mobilidade é exportação estrangeira. Similarmente, verificação para o estado na âncora WLC. O estado do gerente da política deve SER EXECUTADO, e o papel da mobilidade é âncora da exportação.

Configuração de cliente prendida do convidado

O cliente prendido do convidado recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT da saída VLAN mas não pode passar nenhum tráfego até que termine o processo de autenticação da Web.

A fim entrar como um usuário convidado, siga estas etapas:

1. Abra uma janela de navegador e dê entrada com o nome desejado URL (por exemplo, www.cisco.com). O convidado está reorientado ao Web page do padrão do controlador do Wireless LAN se a autenticação da Web é permitida, e uma resolução de DNS pode ser terminada para a URL que é incorporada. Se não, incorpore esta URL: <https://1.1.1.1/login.html>, onde o endereço IP 1.1.1.1 é o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do controlador do Wireless LAN.
2. Incorpore o nome de usuário e senha que é fornecido.

3. Se o início de uma sessão é bem sucedido, notas de uma janela de navegador isso.

Debuga para a conexão prendida do convidado no WLC local

Isto debuga fornece todo o relativo à informação ao cliente prendido do convidado.

```
debug client <mac-address>
```

```
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 â 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.

Troubleshooting

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

Informações Relacionadas

- [Configurando a mobilidade da Auto-âncora](#)
- [Convidado WLAN e WLAN interno usando o exemplo de configuração WLC](#)
- [Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers](#)
- [Manual de configuração do controlador de LAN do Cisco Wireless, liberação 4.2](#)
- [Suporte de produtos Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)