Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers

Contenido

Introducción

Este documento describe cómo configurar el acceso de invitado con el nuevo soporte de característica atado con alambre del acceso de invitado en los controladores de WLAN de Cisco (WLCs) ese Software Release 4.2.61.0 y Posterior del Cisco Unified Wireless del uso. Un número creciente de las compañías reconocen la necesidad de proporcionar el acceso a internet a sus clientes, los Partners, y los consultores cuando visitan sus recursos. Los administradores TIC pueden proporcionar acceso asegurado y controlado atada con alambre y de la Tecnología inalámbrica a Internet para los invitados en el mismo regulador del Wireless LAN.

Los Usuarios invitados deben ser permitidos conectar con los accesos de Ethernet señalados y acceder la red del invitado según lo configurado por el administrador después de que completen los métodos de autentificación configurados. Los Usuarios invitados inalámbricos pueden conectar fácilmente con los controladores de WLAN con las características actuales del acceso de invitado. Además, el sistema de control inalámbrico (WCS), junto con la configuración básica y la Administración de los controladores de WLAN, proporciona los servicios aumentados del Usuario invitado. Para los clientes que han desplegado o planean ya desplegar los controladores de WLAN y el WCS en su red, pueden leverage la misma infraestructura para el acceso de invitado atado con alambre. Esto proporciona una experiencia inalámbrica y atada con alambre unificada del acceso de invitado a los usuarios finales.

Los puertos atados con alambre del invitado se proporcionan en una ubicación señalada y están

conectados en un switch de acceso. La configuración en el switch de acceso pone estos puertos en uno de los VLA N atados con alambre de la capa 2 del invitado. Dos soluciones separadas están disponibles para los clientes:

- Un solo controlador de WLAN (modo de traducción del VLA N) - los trunks del switch de acceso el tráfico atado con alambre del invitado en el VLA N del invitado al controlador de WLAN que proporciona la solución atada con alambre del acceso de invitado. Este regulador realiza la traducción de VLAN del VLA N atado con alambre ingreso del invitado al VLA N de la salida.
- Dos controladores de WLAN (modo auto del ancla) - los trunks del switch de acceso el tráfico atado con alambre del invitado a un controlador de WLAN local (el regulador lo más cerca posible al switch de acceso). Este controlador de WLAN del local asegura al cliente sobre un controlador de WLAN del ancla de la zona desmilitarizada (DMZ) que se configure para el acceso de invitado atado con alambre y inalámbrico. Después de las manos acertadas del cliente al regulador del ancla DMZ, la asignación de la dirección IP del DHCP, autenticación del cliente, y así sucesivamente se maneja en el WLC DMZ. Después de que complete la autenticación, se permite enviar/recibe al cliente el tráfico.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

El soporte de característica atado con alambre del acceso de invitado en los controladores de WLAN de Cisco es soportado por el Software Release 4.2.61.0 y Posterior del Cisco Unified Wireless.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Configuración del switch de capa de acceso

Para proporcionar el acceso de invitado atado con alambre, los puertos señalados en la necesidad del switch de capa de acceso de la capa 2 de ser configurado en el VLA N del invitado por el administrador. El VLA N del invitado debe estar a parte de cualquier otro VLA N que se

configure en este Switch. El tráfico VLAN del invitado es trunked al regulador más cercano del local de la red inalámbrica (WLAN). El regulador del local hace un túnel el tráfico del invitado a través de un Ethernet sobre el túnel IP (EoIP) a un regulador del ancla DMZ. Esta solución requiere por lo menos dos reguladores.

Alternativamente, los trunks del switch de acceso el VLA N del invitado al solo regulador traducen el VLA N del invitado a la interfaz de egreso del 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 la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Puntos importantes para el despliegue atado con alambre del invitado

- Actualmente, cinco soportan al invitado LAN para el acceso de invitado atado con alambre. En el total, 16 WLAN para los usuarios de red inalámbrica y 5 WLAN para el acceso de invitado atado con alambre se pueden configurar en el WLC del ancla. Ningunos túneles diferentes existen para los WLAN. Todo el invitado WLAN, que incluyen los WLAN para el acceso de invitado atado con alambre, utiliza los mismos túneles de EoIP al WLC del ancla.
- Los administradores necesitan crear las interfaces dinámicas en el controlador de WLAN, marcarlas como “invitado LAN,” y asociarlas a los WLAN creados como invitado LAN.
- Asegúrese de que las configuraciones de la red inalámbrica (WLAN), incluyendo la

autenticación, sean idénticas en el ancla y los controladores remotos pasar el tráfico del cliente.
- El WLCs debe tener versiones de software compatibles. Asegúrese de que funcionen con la misma versión importante.
- La autenticación Web es el mecanismo de seguridad predeterminado disponible en un invitado atado con alambre LAN. Las opciones actuales disponibles son éstas: Ábrase, auth de la red, y passthrough de la red.
- En caso del error del túnel de EoIP entre el telecontrol y el WLC del ancla, la base de datos del cliente se limpia del WLC del ancla. El cliente necesita reasociar y reauthenticate.
- No se soporta ninguna Seguridad de la capa 2.
- El Multicast/el tráfico de broadcast en el invitado atado con alambre LAN se cae.
- Las configuraciones de representación del DHCP deben ser idénticas en el ancla y los controladores remotos.

Para el invitado atado con alambre, hay un tiempo de inactividad que se ejecuta en el regulador. Si no se recibe ningunos paquetes dentro del periodo configurado del cliente, quitan al cliente del regulador. Cuando un cliente envía una petición de Address Resolution Protocol (ARP) la próxima vez, una nueva entrada del cliente se crea y se mueve al auth de la red/al estado de funcionamiento apropiadamente según la Configuración de seguridad.

Soporte de la plataforma

El acceso de invitado atado con alambre se soporta en estas Plataformas:

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

Configuración del Wireless LAN

En este ejemplo, la configuración básica del regulador del Wireless LAN se asume. El foco está en la configuración adicional requerida para completar la implementación atada con alambre del acceso de invitado.

1. Cree una interfaz dinámica y marqúela está como “invitado LAN.” Cuando usted crea esta interfaz dinámica en la versión actual, usted necesita proporcionar una dirección IP y un default gateway, aunque no existe puesto que es un VLA N de la capa 2; usted no necesita proporcionar ningún DHCP Address. Los clientes atados con alambre del invitado están conectados físicamente con este VLA N.
2. Cree otra interfaz dinámica donde los clientes atados con alambre del invitado reciben una dirección IP.Nota: Usted necesita proporcionar una dirección IP/a una dirección del servidor del default gateway /DHCP en esta interfaz.
3. Éstas son las interfaces dinámicas:
4. Agregue una nueva red inalámbrica (WLAN): Type=Guest LAN.
5. Habilite la red inalámbrica (WLAN); asocie la interfaz de ingreso al “invitado LAN” creado en el paso 1, y la interfaz de egreso puede ser una interfaz de administración o cualquier otra interfaz dinámica, aunque preferiblemente una interfaz dinámica tal como eso creada en el paso 2.
6. La autenticación Web se habilita por abandono como la opción de seguridad configurada en el invitado LAN. Puede ser cambiada al *passthrough ningunos* o de la *red*.
7. Ésta es la configuración final de la red inalámbrica (WLAN).

8. Agregue a un Usuario invitado en la base de datos local del WLC.En el no nativo, usted necesita fijar el ingreso como el “invitado configurado LAN.” En la salida, usted necesita fijarla a una cierta interfaz, posiblemente la interfaz de administración. Sin embargo, una vez que se construye el túnel de EoIP, envía el tráfico automáticamente a través del túnel en vez de la dirección de administración.

Acceso de invitado atado con alambre con el controlador de WLAN del ancla

En este ejemplo, la dirección IP del regulador remoto del Wireless LAN es 10.10.80.3, y la dirección IP del regulador del ancla DMZ es 10.10.75.2. Ambos son diversos Grupos de movilidad de la parte de dos.

1. Configure al grupo de la movilidad del regulador del ancla DMZ cuando usted agrega la dirección MAC, la dirección IP, y el nombre del grupo de la movilidad del controlador remoto.
2. Semejantemente, configure al grupo de la movilidad en el controlador remoto.
3. Cree la red inalámbrica (WLAN) atada con alambre con el nombre exacto en el WLC del ancla. La interfaz de ingreso en este caso no es “ninguna” porque, lógicamente, la interfaz de ingreso es el túnel de EoIP del controlador remoto. La interfaz de egreso es una diversa interfaz, adonde los clientes atados con alambre van a recibir la dirección IP. En este ejemplo, una interfaz dinámica llamada *invitado* se crea. Sin embargo, usted no puede habilitar en esta etapa la red inalámbrica (WLAN) porque visualiza un mensaje de error, que lee que una interfaz de ingreso no puede ser *ninguna*.
4. Configure la Seguridad de la capa 3 como *autenticación Web*, similar al controlador remoto.
5. Cree el ancla de la movilidad en el regulador del ancla, y asocíela a sí mismo.
6. Una vez que se crea el ancla de la movilidad, vuelva y habilite la red inalámbrica (WLAN) atada con alambre.
7. Semejantemente, cree el ancla de la movilidad en el WLC remoto para la red inalámbrica (WLAN) atada con alambre del invitado.Elija la dirección IP del WLC del ancla y cree el ancla de la movilidad.Marque si los datos y el trayecto de control está para arriba. Si no, asegúrese que estos puertos estén abiertos entre el ancla y el regulador del Wireless LAN del telecontrol: UDP 16666 o IP 97.
8. Una vez que un Usuario invitado atado con alambre está conectado con el Switch y ha completado la autenticación Web, el estado del Administrador de directivas debe SER EJECUTADO, y el papel de la movilidad es exportación no nativa.Semejantemente, comprobación para el estatus en el WLC del ancla. El estado del Administrador de directivas debe SER EJECUTADO, y el papel de la movilidad es ancla de la exportación.

Configuración del cliente atada con alambre del invitado

El cliente atado con alambre del invitado recibe una dirección IP del VLA N de la salida pero no puede pasar ningún tráfico hasta que complete el proceso de autenticación Web.

Para abrir una sesión como Usuario invitado, siga los siguientes pasos:

1. Abra una ventana del buscador y ingrese el nombre deseado URL (por ejemplo, www.cisco.com). Reorientan al invitado al Web page predeterminado del regulador del Wireless LAN si se habilita la autenticación Web, y una resolución de DNS se puede completar para el URL se ingresa que. Si no, ingrese este URL: https://1.1.1.1/login.html,

donde está la dirección IP virtual la dirección IP 1.1.1.1 del regulador del Wireless LAN.

2. Ingrese el nombre de usuario y contraseña se proporciona que.
3. Si el login es acertado, las notas de una ventana del buscador eso.

Debugs para la conexión atada con alambre del invitado en el WLC local

Este debug proporciona todo el relacionado con la información al cliente atado con alambre del invitado.

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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Configurar la movilidad del Auto-ancla
- Ejemplo de Configuración de WLAN Guest y WLAN Interna mediante WLCs
- Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN
- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 4.2
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems