Ejemplo de configuración de controlador de red LAN inalámbrica de Unified Access con anclaje de invitado con acceso convergente

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Configuraciones Parte 1 - Configuración en el 5508 Anchor WLC Parte 2: Configuración de movilidad de acceso convergente entre el WLC serie 5508/5760 y el switch Catalyst serie 3850 Parte 3: Configuración del switch Catalyst serie 3850 externo Verificación Troubleshoot

Introducción

En este documento se describe cómo configurar los controladores de LAN inalámbrica (WLC) de las series 5508/5760 y el switch de la serie Catalyst 3850 para el Guest Anchor del cliente inalámbrico en la nueva configuración de implementación de movilidad, donde el WLC de la serie 5508 actúa como anclaje de movilidad y el switch de la serie Catalyst 3850 actúa como controlador externo de movilidad para los clientes. Además, el switch Catalyst de la serie 3850 actúa como un agente de movilidad para un WLC de la serie 5760 que actúa como un controlador de movilidad desde donde el switch Catalyst de la serie 3850 adquiere la licencia del punto de acceso (AP).

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre estos temas antes de intentar esta configuración:

- GUI o CLI de Cisco IOS[®] con los WLC de acceso convergente de las series 5760 y 3650 y el switch Catalyst serie 3850
- Acceso GUI y CLI con el WLC serie 5508
- Configuración del identificador del conjunto de servicios (SSID)
- Autenticación Web

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5760 versión 3.3.3 (sala de cableado de última generación [NGWC])
- Catalyst 3850 Series Switch
- WLC de la serie 5508 de Cisco versión 7.6.120
- Puntos de acceso ligeros de Cisco serie 3602
- Cisco Catalyst 3560 Series Switches

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Nota: Use el <u>Command Lookup Tool</u> (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

El WLC de la serie 5508 actúa como un controlador de anclaje, y el switch Catalyst de la serie 3850 actúa como un controlador externo y el agente de movilidad que obtiene la licencia del controlador de movilidad 5760.



Nota: En el diagrama de red, el WLC de la serie 5508 actúa como controlador de anclaje, el WLC de la serie 5760 actúa como controlador de movilidad y el switch de la serie Catalyst 3850 actúa como agente de movilidad y WLC externo. En cualquier momento, el controlador de anclaje para el switch Catalyst de la serie 3850 es el WLC de la serie 5760 o el WLC de la serie 5508. Ambos no pueden ser anclajes al mismo tiempo, porque el doble anclaje no funciona.

Configuraciones

La configuración consta de tres partes:

Parte 1 - Configuración en el 5508 Anchor WLC

Parte 2 - Configuración de Movilidad de Acceso Convergente entre el WLC 5508/5760 Series y el Catalyst 3850 Series Switch

Parte 3: Configuración en el switch Catalyst serie 3850 externo

Parte 1 - Configuración en el 5508 Anchor WLC

1. En el WLC de la serie 5508, pase el cursor sobre WLAN > New para crear una nueva LAN

inalámbrica (WLAN).

| MONITOR WLANS COL | NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP |
|---------------------------------|---|
| WLANs > Edit 'CUW | N' |
| General Security | QoS Policy-Mapping Advanced |
| Profile Name | CUWN |
| Туре | WLAN |
| SSID | CUWN |
| Status | Enabled |
| Security Policies | WEB POLICY, Web-Auth (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | vlan60 👻 |
| Multicast Vlan Feature | C Enabled |
| Broadcast SSID | Enabled |
| NAS-ID | 5508 |
| | MONITOR WLANS CO WLANS > Edit 'CUW General Security Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID |

2. Pase el ratón sobre WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication para configurar Layer 3 Security.

| | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBA |
|------------------|--|
| WLANs | WLANs > Edit 'CUWN' |
| ▼ WLANs WLANs | General Security QoS Policy-Mapping Advanced |
| Advanced | Layer 2 Layer 3 AAA Servers |
| | Layer 3 Security ² Web Policy 👻 |
| | Authentication Passthrough |
| | Conditional Web Redirect |
| | Splash Page Web Redirect On MAC Filter failure ¹⁰ |
| | Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None |
| | Sleeping Client 🔲 Enable |
| | Over-ride Global Config 🔲 Enable |

3. Haga que la dirección de anclaje sea **local** en la ventana de configuración de anclaje de movilidad WLAN para agregar el WLC de la serie 5508 como anclaje.

| | | | | | | | | | | Sa⊻e Configural |
|------------|---------------|------------|----------|----------|------------|----------|------|----------|-----------|---------------------|
| MONITOR | <u>W</u> LANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | EEEDBACK | | |
| Mobility # | hchors | | | | | | | | | |
| WLAN SSI | D CUM | TN . | | | | | | | | |
| Switch IP | Address (| Anchor) | | | | | | | Data Path | Control Path |
| local | | | | | | | | | up | up |
| Mobility | Anchor Cr | eate | | | | | | | | |

4. Pase el ratón sobre la **página Security > Webauth > Webauth** para configurar la página Webauth que se utilizará para la autenticación del cliente.

En este ejemplo, se selecciona la página WLC Internal Webauth:

| cisco | | WLANs | | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | EEEDBACK |
|--|---|--------|--|--|---|---------------------------|----------|------|----------|
| Security | Web Logi | n Page | | | | | | | |
| AAA General RADIUS Authentication Accounting Fallback Due | Web Authentication Type Redirect URL after login This page allows you to customize the content a page. The Login page is presented to web users WLAN if "Web Authentication" is turned on (unde | | | Inter Intert and appe b users the first (under WLAN : | mal (Default) arance of the I time they acc Security Policie | Login ress the es). | • | |] |
| DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies | Cisco Logo Show C Headline Message | | | | | | | | |

5. Cree un usuario de red local. El usuario utiliza este par de nombre de usuario y contraseña cuando se le solicita en la página Webauth.

| cisco | MONITOR WLANS | | WIRELESS | SECURITY | MANAGEMENT | с <u>о</u> |
|--|---|----------------|---------------------------------|----------|------------|------------|
| Security | Local Net Users > | Edit | | | | |
| AAA General RADIUS Authentication | User Name Password | surbg | | | | |
| Authentication Accounting Fallback DNS | Confirm Password Creation Time Remaining Time | Mon N N/A | Mon May 19 12:00:41 2014 N/A | | | |
| LDAP Local Net Users MAC Filtering | WLAN Profile Description | Any V surbg | VLAN 🔻 | | | |

Parte 2: Configuración de movilidad de acceso convergente entre el WLC serie 5508/5760 y el switch Catalyst serie 3850

1. En el WLC de la serie 5508, agregue el WLC de la serie 5760 como el par de la movilidad.

| cisco | MONITOR WLANS CO | ONTROLLER WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | EEEOBACK | _ | | 8 |
|--|-----------------------|--------------------|----------|------------|------------|--------|----------|--------------|----|--------|
| Controller | Static Mobility Group | Members | | | | | | | | |
| General Inventory | Local Nobility Group | Mobile-1 | | | | | | | | |
| Interfaces | NAC Address | IP Address | | Public | IP Address | Group | Name | Nulticast IP | | itatus |
| Interface Groups | 58:8d:09:cd:ac:60 | 10.105.135.151 | | 10.105 | 135.151 | Mobile | -1 | 0.0.0.0 | U | ip. |
| Multicast | 02-00-00-00-00-00 | 10.105.105.170 | | | | | | | | - |
| Network Routes | 00:00:00:00:00:00 | 10.105.135.178 | | 10.109 | 135.178 | surag | | 0.0.0.0 | U. | .p |
| Redundancy | 00:00:00:00:00:00 | 10.105.135.244 | | 10.105 | 135.244 | surag | | 0.0.0.0 | | P |
| Internal DHCP Server | | | | | | | | | | |
| Mobility Management Mobility Configuration Mobility Groups | | | | | | | | | | |

2. En el WLC de la serie 5760, que actúa como controlador de la movilidad, agregue el WLC de la serie 5508 como el par de la movilidad.

| cificație cisco Wireless Controller | 🛆 Home | Monitor • Configuration | Administration • | нер | | |
|--|----------------|---------------------------|--------------------|--------------|---------------------|------------------|
| Controller | Mobility Peer | | | | | |
| * 🧰 System | New Remove | | | | | |
| General | IP Address | Public IP Address | Group Name | Multicast IP | Control Link Status | Data Link Status |
| Multicast | 10.105.135.244 | | gubg | 0.0.0.0 | | - |
| Interfaces | 10.105.135.151 | 10.105.135.151 | Mobile-1 | | UP | UP |
| VLAN | 10.105.135.178 | 10.105.135.178 | gdrue | 0.0.0.0 | UP | UP |
| Internal DHCP Server | | | | | | |
| Management | | | | | | |
| * 😂 Mobility Management | | | | | | |
| Mobility Global Config Mobility Rear Switch Peer Group | | | | | | |

 ¡Este paso es muy importante! Agregue el Catalyst 3850 Series Switch como el agente de movilidad en el WLC de la serie 5760 en la pestaña Switch Peer Group bajo Mobility Management.

| ultatia cisco Wireless Controller | <u> </u> | Configuration Administr | ation i 🔻 Help | |
|--------------------------------------|--|-----------------------------|---------------------|------------------|
| Controller | Switch Peer Group > SURBG-SPG Switch Peer Group > SURBG-SPG | | | |
| 📲 🔤 System | | | | |
| General | New Remove | | | |
| Multicast | IP Address | Public IP Address | Control Link Status | Data Link Status |
| Interfaces | 10.105.135.226 | 10.105.135.226 | UP | UP |
| VLAN | | | | |
| Internal DHCP Server | | | | |
| Management | | | | |
| Mobility Management | | | | |
| Mobility Global Config | | | | |
| Mobility Peer | | | | |
| Switch Peer Group | | | | |

4. En el switch Catalyst de la serie 3850, agregue el WLC de la serie 5760 como el controlador de movilidad. Una vez hecho esto, el switch Catalyst serie 3850 obtiene la licencia de AP Cloud del controlador de movilidad 5760.

| 🟡 Home | Monitor 🔻 | Configuration 🔻 | Administration |
|----------------------------------|---|---|--|
| Mobility Agent Configurat | tion | | |
| | | | |
| Mobility Role | | Mobility Agent 💌 | |
| Mobility Controller IP Address | • | 10.105.135.244 | |
| Control Link Status | | UP | |
| Data Link Status | | UP | |
| Mobility Protocol Port | | 16666 | |
| Mobility Switch Peer Group Na | ame <mark>.</mark> | SURBG-SPG | |
| DTLS Mode | | Enabled | |
| Mobility Domain ID for 802.11 | r | 0xe699 | |
| Mobility Keepalive Interval (1-3 | 30)sec | 10 | |
| | Mobility Agent Configurat Mobility Role Mobility Controller IP Address Control Link Status Data Link Status Mobility Protocol Port Mobility Switch Peer Group Na DTLS Mode Mobility Domain ID for 802.111 Mobility Keepalve Interval (1-1) | Image: None Monitor Mobility Agent Configuration Mobility Role Mobility Controller IP Address Mobility Controller IP Address Control Link Status Data Link Status Mobility Protocol Port Mobility Switch Peer Group Name DTLS Mode Mobility Domain ID for 802.11r Mobility Keepalive Interval (1-30)sec | Mobility Agent Configuration Mobility Agent Configuration Mobility Role Mobility Controller IP Address Mobility Controller IP Address Control Link Status Control Link Status UP Data Link Status Mobility Protocol Port Mobility Switch Peer Group Name DTLS Mode Mobility Domain ID for 802.11r Mobility Keepalive Interval (1-30)sec 10 |

Parte 3: Configuración del switch Catalyst serie 3850 externo

1. Pase el ratón sobre **GUI > Configuration > Wireless > WLAN > New** para configurar el SSID/WLAN exacto en el switch Catalyst de la serie 3850.

| սիսիս | | |
|---------------------------|-----------------------------|---|
| CISCO Wireless Controller | 🏠 Home | Monitor Configuration Administration Help |
| Wireless | WLAN > Edit | |
| | General Security | QOS AVC Policy Mapping Advanced |
| Access Points | Profile Name | CUWN |
| B02.11a/n/ac | Туре | WLAN |
| B02.11b/g/n | SSID | CUWN |
| Media Stream | Status | Enabled |
| • QOS | Security Policies | Web-Auth (Modifications done under security tab will appear after applying the changes.) |
| | Radio Policy | AI V |
| | Interface/Interface Group(G | ;) VLAN0060 🔎 |
| | Broadcast SSID | |
| | Multicast VLAN Feature | |

2. Pase el ratón sobre WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication para configurar Layer 3 Security.

| սիսիս | | | | |
|--|--|------------------------------|-----------------------|----------------|
| cisco Wireless Controller | 🏡 Home | Monitor 🛛 🔹 Cor | nfiguration 💌 Adminis | tration 🔻 Help |
| Wireless | WLAN > Edit | | | |
| WLAN WLAN Access Points | General Security Layer2 Layer3 | QOS AV | /C Policy Mapping | Advanced |
| 802.11a/n/ac 802.11b/g/n Media Stream OOS | Web Policy Conditional Web Redirect Webauth Authentication Li Webauth Parameter Map | ist Disabled | م م | |
| | Webauth On-mac-filter Fail Preauthentication IPv4 AC Preauthentication IPv6 AC | ure L Unconfigu L none | red 🔎 | |

3. Agregue la dirección IP del WLC de la serie 5508 como anclaje en la configuración del anclaje de movilidad de WLAN

| cisco Wireless Controller | Administration ▼ Help Administration ▼ Help |
|---|--|
| Wireless | Mobility Anchors WLAN > Edit |
| WLAN WLANs Access Points 802.11a/n/ac | WLAN Profile QUWN Switch IP Address Create Mobility Anchor |
| Media Stream QOS | Remove Anchor IP Address 10.105.135.151 |

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Conecte el cliente a la red inalámbrica unificada de Cisco (CUWN) WLAN. Este es el flujo de trabajo:

- 1. El cliente recibe una dirección IP.
- 2. El cliente abre un navegador y accede a cualquier sitio web.
- 3. El primer paquete TCP enviado por el cliente es secuestrado por el WLC, y el WLC intercepta y envía la página Webauth.
- 4. Si el DNS está configurado correctamente, el cliente obtiene la página Webauth.
- 5. El cliente debe proporcionar el nombre de usuario/contraseña para autenticarse.
- 6. Después de una autenticación exitosa, el cliente es redirigido a la página de acceso original.

|) 🦉 https://19 | 2.168.200.1 🔎 👻 C. 🛽 | े 🖒 🗙 🥖 Web Authentica | ition × |
|---|---|---|---------|
| Login | | | |
| Welcome to | the Cisco wireless | network | |
| Cisco is pleased our network. Ple solution to work. | to provide the Wireless L ase login and put your uni | AN infrastructure for ified wireless | |
| Jser Name | | | |
| Password | | | |
| | Submit | | |
| | | | |

7. Después de que el cliente proporciona las credenciales correctas, el cliente pasa la autenticación.

| æ | → http://www.google.com/ P → ♂ × | Internet Explorer cannot dis × |
|---|--|--------------------------------|
| Ş | Cogout - Windows Internet Explorer | × vebpage |
| | Web Authentication Login Successful ! You can now use all regular network services over the wireless network. | |
| | Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: <u>https://192.168.200.1/logout.html</u> Logout | - |
| | a 100% | |

Troubleshoot

Para resolver problemas de su configuración, ingrese estos debugs en el WLC de la serie 5508, que actúa como anclaje de invitado:

Debug Client

```
Debug web-auth redirect enable mac
```

Aquí tiene un ejemplo:

Debug Client 00:17:7C:2F:B6:9A Debug web-auth redirect enable mac 00:17:7C:2F:B6:9A

show debug

MAC Addr 1..... 00:17:7C:2F:B6:9A

Debug Flags Enabled: dhcp packet enabled. dot11 mobile enabled. dot11 state enabled dot1x events enabled. dot1x states enabled. FlexConnect ft enabled. pem events enabled. pem state enabled. CCKM client debug enabled. webauth redirect enabled.

*mmMaListen: May 19 13:36:34.276: 00:17:7c:2f:b6:9a Adding mobile on Remote AP 00:00:00:00:00(0)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override for default ap group, marking intgrp NULL *mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Applying Interface policy on Mobile, role Unassociated. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 0

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Re-applying interface policy for client

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2219) *mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2240) *mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type *mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override from intf group to an intf for roamed client - removing intf group from mscb

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 acl from
255 to 255
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 Flex acl
from 65535 to 65535
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Stopping deletion of Mobile
Station: (callerId: 53)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Adding
Fast Path rule type = Airespace AP - Learn IP address
on AP 00:00:00:00:00, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path
rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60,
Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) State
Update from Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor,
client state=APF_MS_STATE_ASSOCIATED
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Change state to DHCP_REQD (7) last state DHCP_REQD (7)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 5807, Adding TMP rule
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
type = Airespace AP - Learn IP address
on AP 00:00:00:00:00, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local
Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Sent an XID frame
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Pushing IPv6 Vlan Intf
ID 13: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A ,
Binding to Data Plane. SUCCESS !! dhcpv6bitmap 0
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Calling mmSendIpv6AddrUpdate
for addition of IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , for MAC:
00:17:7C:2F:B6:9A
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a mmSendIpv6AddrUpdate:4800
Assigning an IPv6 Addr fe80:0000:0000:0000:6c1a:b253:d711:0c7f to the client in
Anchor state update the foreign switch 10.105.135.226
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Link Local address fe80::
6c1a:b253:d711:c7f updated to mscb. Not Advancing pem state.Current state: mscb
in apfMsMmInitial mobility state and client state APF_MS_STATE_AS
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
 type = Airespace AP - Learn IP address
```

on AP 00:00:00:00:00, slot 0, interface = 1, QOS = 0 IPv4 ACL ID = 255, *mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60, Local Bridging intf id = 13 *mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255) *pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a Set bi-dir quest tunnel for 00:17:7c:2f:b6:9a as in Export Anchor role *pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x4 *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Static IP client associated to interface vlan60 which can support client subnet. *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7) *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) pemAdvanceState2 6717, Adding TMP rule *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) Replacing Fast Path rule type = Airespace AP Client - ACL passthru on AP 00:00:00:00:00, slot 0, interface = 1, QOS = 0 IPv4 ACL *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60, Local Bridging intf id = 13 *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255) *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Plumbing web-auth redirect rule due to user logout *dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a apfAssignMscbIpAddr:1148 Assigning an Ip Addr 60.60.60.11 to the client in Anchor state update the foreign switch 10.105.135.226 *dtlArpTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Assigning Address 60.60.60.11 to mobile *pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for 00:17:7c:2f:b6:9a as in Export Anchor role *pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a 60.60.60.11 Added NPU entry of type 2, dtlFlags 0x4 *pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Pushing IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A , Binding to Data Plane. SUCCESS !! *pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Sent an XID frame (5508-MC) > (5508-MC) > (5508-MC) >*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP received op BOOTREQUEST (1) (len 314, vlan 0, port 1, encap 0xec07) *DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07) mstype 3ff:ff:ff:ff:ff *DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a 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 *DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selected relay 1 -60.60.251 (local address 60.60.60.2, gateway 60.60.251, VLAN 60, port 1) *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP REOUEST (3) *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1 *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3 (2902502819), secs: 3072, flags: 0 *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP chaddr: 00:17:7c:2f:b6:9a

*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0, giaddr: 60.60.60.2 *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP requested ip: 60.60.60.11 *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP sending REQUEST to 60.60.60.251 (len 358, port 1, vlan 60) *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selecting relay 2 control block settings: dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 60.60.60.2 VLAN: 60 *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selected relay 2 -NONE (server address 0.0.0.0,local address 0.0.0.0, gateway 60.60.60.251, VLAN 60, port 1) *DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP received op BOOTREPLY (2) (len 308, vlan 60, port 1, encap 0xec00) *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP setting server from ACK (server 60.60.60.251, yiaddr 60.60.60.11) *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP ACK (5) *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3 (2902502819), secs: 0, flags: 0 *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP chaddr: 00:17:7c:2f:b6:9a *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0, yiaddr: 60.60.60.11 *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 *DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP server id: 192.168.200.1 rcvd server id: 60.60.60.251 *webauthRedirect: May 19 13:36:47.678: 0:17:7c:2f:b6:9a- received connection *webauthRedirect: May 19 13:36:47.680: captive-bypass detection disabled, Not checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Preparing redirect URL according to configured Web-Auth type *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Checking custom-web config for WLAN ID:4 *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- unable to get the hostName for virtual IP, using virtual IP =192.168.200.1 *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Global status is enabled, checking on web-auth type *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type Internal, no further redirection needed. Presenting defualt login page to user *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http response msg body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv= "Cache-control" content="no-cache"><META http-equiv="Pragma" content="n *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body2 is "></HEAD></HTML> *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser host is www.facebook.com

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser path is /
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- added redirect=,
URL is now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 312

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Message to be sent is HTTP/1.1 200 OK Location: https://192.168.200.1/login.html?redirect=www.facebook.com/ Content-Type: text/html Content-Length: 312 <HTML><HEAD *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- send data length=448 *webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type External, but unable to get URL *webauthRedirect: May 19 13:36:47.681: 0:17:7c:2f:b6:9a- received connection *emWeb: May 19 13:36:48.731: SSL Connection created for MAC:0:17:7c:2f:b6:9a *webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- received connection *webauthRedirect: May 19 13:36:51.795: captive-bypass detection disabled, Not checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a *webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- Preparing redirect URL according to configured Web-Auth type *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Checking custom-web config for WLAN ID:4 *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- unable to get the hostName for virtual IP, using virtual IP =192.168.200.1 *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Global status is enabled, checking on web-auth type *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type Internal, no further redirection needed. Presenting defualt login page to user *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv= "Cache-control" content="no-cache"><META http-equiv="Pragma" content="n *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body2 is "></HEAD></HTML> *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser host is www.facebook.com *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser path is /favicon.ico *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- added redirect=, URL is now https://192.168.200.1/login.html? *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- str1 is now https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- clen string is Content-Length: 323 *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Message to be sent is HTTP/1.1 200 OK Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico Content-Type: text/html Content-Length: 323 *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- send data length=470 *webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type External, but unable to get URL *DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP received op BOOTREQUEST (1) (len 308, vlan 0, port 1, encap 0xec07) *DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07) mstype 3ff:ff:ff:ff:ff *DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP selecting relay 1 control block settings:

dhcpServer: 60.60.60.251, dhcpNetmask: 255.255.255.0, dhcpGateway: 60.60.60.251, dhcpRelay: 60.60.60.2 VLAN: 60

```
*emWeb: May 19 13:38:35.187:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1
```

```
*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:47.215:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1
```

```
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created in mscb for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD
(8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)
```

```
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a apfMsRunStateInc
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_NOL3SEC
(14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)
```

```
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Session Timeout is 0 -
not starting session timer for the mobile
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Reached PLUMBFASTPATH: from line 6605
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Replacing Fast Path rule
```

```
type = Airespace AP Client
```

```
on AP 00:00:00:00:00, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv6 ACL ID =
```

Esta es la captura de paquetes del lado del cliente.

El cliente obtiene la dirección IP.

| Smartlin_2f:b6:9a | Broadcast | ARP | 42 who has 60.60.60.11? Tell 0.0.0.0 |
|--------------------------|-----------------|------------|--|
| Smartlin_2f:b6:9a | Broadcast | ARP | 42 who has 60.60.60.251? Tell 60.60.60.11 |
| Smartlin_2f:b6:9a | Broadcast | ARP | 42 Gratuitous ARP for 60.60.60.11 (Request) |
| 0.0.0.0 | 255.255.255.255 | DHCP | 348 DHCP Request - Transaction ID 0xd73b645b |
| 192.168.200.1 | 60.60.60.11 | DHCP | 346 DHCP ACK - Transaction ID 0xd73b645b |
| Automatic strategies and | ££65 | T CHIP: 10 | Construction of the second sec |

El cliente abre un navegador y escribe www.facebook.com.

| | | | the second second and any second second second second |
|--|-----------------|-----|---|
| 60.60.60.11 | 50.50.50.251 | DNS | 76 Standard query 0x18bc A www.facebook.com |
| 50.50.50.251 | 60.60.60.11 | DNS | 92 Standard query response 0x18bc A 56.56.56.56 |
| 60.60.60.11 | 50.50.50.251 | DNS | 76 Standard query Oxab1b AAAA www.facebook.com |
| 60.60.60.11 | 50.50.50.251 | DNS | 76 Standard query Oxab1b AAAA www.facebook.com |
| 60.60.60.11 | 50, 50, 50, 251 | DNS | 76 Standard query Oxab1b _ AAAA_www.facebook.com |
| < | | | |
| | | | |
| 🛚 Frame 508: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0 | | | |
| Ethernet II, Src: Smartlin_2f:b6:9a (00:17:7c:2f:b6:9a), Dst: Cisco_fc:96:a8 (f0:f7:55:fc:96:a8) | | | |
| Internet Protocol Version 4, Src: 60.60.60.11 (60.60.60.11), Dst: 50.50.50.251 (50.50.251) | | | |
| B User Datagram Protocol, Src Port: 62672 (62672), Dst Port: domain (53) | | | |

```
Domain Name System (query)
```

```
Transaction ID: 0xablb
```

```
Flags: 0x0100 Standard query
Questions: 1
Answer RRS: 0
Authority RRS: 0
Additional RRS: 0
```

```
Queries
```

www.facebook.com: type AAAA, class IN

El WLC intercepta el primer paquete TCP del cliente y envía su dirección IP virtual y la página de Webauth interna.

| 56.56.56.56 | 60.60.60.11 | TCP | 54 http > 49720 [ACK] seq=1 Ack=207 win=6656 Len=0 | | |
|--|------------------------|-----------------------------|--|--|--|
| 56.56.56.56 | 60.60.60.11 | HTTP | 524 HTTP/1.1 200 OK (text/html) | | |
| 56 56 56 56 | 60 60 60 11 | TCP | 54 http://wine6656.jene0 | | |
| 4 | | | | | |
| ■ Frame 550: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface 0 | | | | | |
| Ethernet II, | Src: Cisco_fc:96:a8 (| f0:f7:55:fc:96:a8), Dst: Sm | artlin_2f:b6:9a (00:17:7c:2f:b6:9a) | | |
| Internet Protocol Version 4, Src: 56.56.56.56.56.56.56.56.56, Dst: 60.60.60.11 (60.60.60.11) | | | | | |
| In Transmission Control Protocol, Src Port: http (80), Dst Port: 49720 (49720), Seq: 1, Ack: 207, Len: 470 | | | | | |
| Hypertext Tra | ansfer Protocol | | | | |
| HTTP/1.1 20 | 00 ok\r\n | | | | |
| Location: A | https://192.168.200.1/ | login.html?redirect=www.fac | ebook.com/favicon.ico\r\n | | |
| Content-Type: text/html\r\n | | | | | |
| E Content-Length: 323\r\n | | | | | |
| \r\n | \r\n | | | | |
| [HTTP respo | onse 1/1] | | | | |

[HTTP response 1/1]

Después de una autenticación web correcta, se completa el resto del flujo de trabajo.

| 60.60.60.11 | 50.50.50.251 | DNS | 86 Standard query 0x64dd A 1e9cvlist,ie.microsoft.com |
|---------------|---------------|----------|---|
| 60.60.60.11 | 192.168.200.1 | TCP | 66 49724 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=4 SACK_PERM=1 |
| 192.168.200.1 | 60.60.60.11 | TCP | 66 https > 49724 [SYN, ACK] Seq=0 Ack=1 Win=5560 Len=0 MSS=1390 SACK_PERM=1 WS=64 |
| 60.60.60.11 | 192.168.200.1 | TCP | 54 49724 > https [ACK] Seq=1 Ack=1 win=16680 Len=0 |
| 60.60.60.11 | 192,168,200,1 | TLSV1 | 190 client Hello |
| 192.168.200.1 | 60.60.60.11 | TCP | 54 https > 40724 [ACK] Seq=1 Ack=137 W1n=6656 Len=0 |
| 192.168.200.1 | 60.60.60.11 | TLSV1 | 192 Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 60.60.60.11 | 192.168.200.1 | TLSV1 | 113 Change Cipher Spec, Encrypted Handshake Message |
| 60.60.60.11 | 50.50.50.251 | DNS | 83 Standard query 0xb814 A ctldl.windowsupdate.com |
| 192.168.200.1 | 60.60.60.11 | TCP | 54 https > 49724 [ACK] Seq=139 Ack=196 win=6656 Len=0 |
| 60 60 60 33 | 40 40 40 315 | A STATUT | 63 Mars Hundre ND TEATAD 60. |

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).