통합 액세스 컨피그레이션이 포함된 Unified Access Wireless LAN Controller 게스트 앵커 예

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 구성 네트워크 다이어그램 설정 1부 - 5508 앵커 WLC의 컨피그레이션 2부 - 5508/5760 Series WLC와 Catalyst 3850 Series Switch 간의 통합 액세스 모빌리티 구성 3부: Foreign Catalyst 3850 Series 스위치의 구성 다음을 확인합니다. 문제 해결

소개

이 문서에서는 5508 Series WLC가 모빌리티 앵커 역할을 하고 Catalyst 3850 Series 스위치가 클라 이언트의 모빌리티 외부 컨트롤러 역할을 하는 새로운 모빌리티 구축 설정에서 무선 클라이언트 게 스트 앵커에 대해 5508/5760 Series WLC(Wireless LAN Controller) 및 Catalyst 3850 Series 스위치 를 구성하는 방법에 대해 설명합니다. 또한 Catalyst 3850 Series Switch가 Mobility Agent 역할을 하 여 Catalyst 3850 Series Switch가 Access Point(AP) 라이센스를 획득하는 5760 Series WLC에서 Mobility Controller 역할을 합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco IOS[®] GUI 또는 CLI(Converged Access 5760 및 3650 Series WLC 및 Catalyst 3850 Series 스위치 포함)
- 5508 Series WLC를 통한 GUI 및 CLI 액세스
- SSID(Service Set Identifier) 컨피그레이션
- 웹 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 5760 릴리스 3.3.3(NGWC[Next Generation Wiring Closet])
- Catalyst 3850 Series 스위치
- Cisco 5508 Series WLC 릴리스 7.6.120
- Cisco 3602 Series Lightweight AP
- Cisco Catalyst 3560 Series Switches

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

참고: 이 섹션에서 사용된 <u>명령에</u> 대한 자세한 내용을 보려면<u>Command Lookup Tool(등록된</u> 고객만 해당)을 사용하십시오.

네트워크 다이어그램

5508 Series WLC는 앵커 컨트롤러 역할을 하며, Catalyst 3850 Series 스위치는 Foreign Controller 및 Mobility Controller 5760에서 라이센스를 얻은 Mobility Agent 역할을 합니다.



참고: 네트워크 다이어그램에서 5508 Series WLC는 앵커 컨트롤러, 5760 Series WLC는 모 빌리티 컨트롤러, Catalyst 3850 Series 스위치는 모빌리티 에이전트 및 외부 WLC 역할을 합 니다. 어느 시점에서든 Catalyst 3850 Series Switch의 Anchor Controller는 5760 Series WLC 또는 5508 Series WLC입니다. 이중 앵커가 작동하지 않기 때문에 두 앵커가 동시에 앵커가 될 수 없습니다.

설정

이 구성에는 세 가지 부분이 포함됩니다.

<u>1부 - 5508 앵커 WLC의 컨피그레이션</u>

<u>2부 - 5508/5760 Series WLC와 Catalyst 3850 Series Switch 간의 Converged Access Mobility</u> <u>Configuration</u>

<u> 3부 - Foreign Catalyst 3850 Series 스위치의 구성</u>

1부 - 5508 앵커 WLC의 컨피그레이션

1. 5508 Series WLC에서 새 무선 LAN(**WLAN)**을 생성하려면 WLAN(WLAN) > New(새로 만들기)에 마우스를 놓습니다.

cisco	MONITOR WLANS COL	NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit 'CUW	4'
✓ WLANS WLANS	General Security	QoS Policy-Mapping Advanced
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	Enabled
	Broadcast SSID	Enabled
	NAS-ID	5508
	149-10	3300

2. 레이어 3 보안을 **구성하려면 WLAN > WLAN Edit > Security > Layer 3 enabled Web**authentication 위에 마우스 커서를 놓습니다.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBA
WLANs	WLANs > Edit 'CUWN'
 ₩LANs WLANs Advanced 	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers
	Layer 3 Security ⁴ 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. 5508 Series WLC를 앵커로 추가하려면 WLAN mobility Anchor 컨피그레이션 창 아래에서 앵 커 주소를 로컬로 설정합니다.

										Sa <u>v</u> e Configura
MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK		
Mobility A	Inchors									
WLAN SSI	D CUW	N								
Switch IP	Address (Anchor)							Data Path	Control Path
local									up	υρ
Mobility	Anchor Cr	eate								

- 4. Security(보안) > Webauth(웹 인증) > Webauth(웹 인증) 페이지 위에 마우스 커서를 올려 놓으 면 클라이언트 인증에 사용할 웹 인증 페이지를 구성할 수 있습니다.
 - 이 예에서는 WLC 내부 웹 인증 페이지가 선택됩니다.

ı. cısco		WLANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK
Security	Web Log	in Page	Туре	Inte	mal (Default)		•		
■ RADIUS Authentication Accounting Fallback DNS	Redirect URL after login This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if "Web Authentication" is turned on (under WLAN Security Policies).]		
▶ TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Cisco Log Headline Message	10	Sho	w OHide					

5. 로컬 네트워크 사용자를 생성합니다. 이 사용자 이름/비밀번호 쌍은 Webauth 페이지에 프롬 프트가 표시되면 사용자가 사용합니다.

cisco	MONITOR <u>W</u> LANS		WIRELESS	SECURITY	MANAGEMENT	с <u>о</u>
Security	Local Net Users >	Edit				
▼ AAA General	User Name	surbg				
- RADIUS	Password	•••				
Authentication	Confirm Password	•••				
Fallback	Creation Time	Mon M	lay 19 12:00:4	1 2014		
DNS	Remaining Time	N/A				
LDAP	WLAN Profile	Any V	VLAN 👻			
Local Net Users	Description	surbg				
MAC Filtering						

2부 - 5508/5760 Series WLC와 Catalyst 3850 Series Switch 간의 통합 액세스 모빌리티 구성

1. 5508 Series WLC에서 5760 Series WLC를 모빌리티 피어로 추가합니다.

uluili. cisco	MONITOR WLANS CO	INTROLLER WIRELESS SECU	NTY MANAGEMENT	COMMANDS	HELP EEEDBACK		\$
Controller	Static Mobility Group	Members					
General Inventory	Local Nobility Group	Mobile-1					
Interfaces	MAC Address	IP Address	Publi	c IP Address	Group Name	Multicast IP	Status
Interface Groups	58:8d:09:cd:ac:60	10.105.135.151	10.10	6.135.151	Mobile-1	0.0.0.0	Up
Multicast							
Network Routes	00:00:00:00:00:00	10.105.135.170	10.10	6.135.178	surbg	0.0.0.0	Up
h Badandance	00:00:00:00:00:00	10.105.135.244	10.10	6.135.244	eurbg	0.0.0.0	Up
Internal DHCP Server							
 Mobility Management Mobility Configuration Nobility Groups 							

2. 5760 Series WLC에서 모빌리티 컨트롤러 역할을 하면서 5508 Series WLC를 모빌리티 피어 로 추가합니다.

altada Cisco Wireless Controller	A Home	Monitor • Configurat	ion 🔹 Administration I 🔹	нар		
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		subg	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 Page Switch Peer Group						

3. 이 단계는 매우 중요합니다! Mobility Management(모빌리티 관리) 아래의 Switch Peer Group(스위치 피어 그룹) 탭 아래에 있는 5760 Series WLC에서 Catalyst 3850 Series 스위치 를 모빌리티 에이전트로 추가합니다.

cisco Wireless Controller	☆ Home Manitor	Configuration Administr	ation I 💌 Help	
Controller	Switch Peer Group > SURBG-SPG Switch Peer Group > SURBG-SPG			
▼ 🚘 System	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. Catalyst 3850 Series Switch에서 5760 Series WLC를 모빌리티 컨트롤러로 추가합니다. 이렇 게 하면 Catalyst 3850 Series Switch가 Mobility Controller 5760에서 AP 클라우드 라이센스를 획득합니다.

ahah				
cisco Wireless Controller	🏠 Home	Monitor 🛛 🔻	Configuration •	Administration
Controller	Mobility Agent Configura	tion		
▼ 📴 System				
General	Mobility Role		Mobility Agent 💌	
Multicast	Mobility Controller IP Address	•	10.105.135.244	
Interfaces	Control Link Status		UP	
VLAN	Data Link Status		UP	
🕨 🧰 Internal DHCP Server	Mobility Protocol Port		16666	
🕨 🧰 Management	Mobility Switch Peer Group Na	ame <mark>.</mark>	SURBG-SPG	
🔻 🚘 Mobility Management	DTLS Mode		Enabled	
Mobility Global Config	Mobility Domain ID for 802.11	1	Oxe699	
Mobility Peer	Mobility Keepalive Interval (1-	30)sec	10	

3부: Foreign Catalyst 3850 Series 스위치의 구성

1. Catalyst 3850 Series 스위치에서 정확한 SSID/WLAN을 구성하려면 GUI > Configuration > Wireless > WLAN > New 위에 마우스 커서를 올려 놓습니다.

2. 레이어 3 보안을 **구성하려면 WLAN > WLAN Edit > Security > Layer 3 enabled Web**authentication 위에 마우스 커서를 놓습니다.

սիսիս	
cisco Wireless Controller	🏡 Home Monitor I▼ Configuration I▼ Administration I▼ Help
	WLAN WLAN > Edit
VLANs Access Points	Layer2 Layer3 AAA Server
 802.11a/n/ac 802.11b/g/n Media Stream 	Web Policy Conditional Web Redirect Webauth Authentication List Disabled
> 🦲 QOS	Webauth Parameter Map web Presetthentication IPv4 ACL Preauthentication IPv6 ACL none

3. WLAN Mobility Anchor 컨피그레이션에서 5508 Series WLC IP 주소를 앵커로 추가합니다

cisco Wireless Controller	Administration ▼ Help
Wireless WLAN WLAN Access Points 302.11a/n/ac 302.11b/g/n Media Stream QOS	Mobility Anchors WLAN > Edit WLAN Profile QUWN Switch IP Address Create Mobility Anchor Remove Anchor IP Address IP Address 10.105.135.151

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

클라이언트를 WLAN CUWN(Cisco Unified Wireless Network)에 연결합니다. 워크플로는 다음과 같 습니다.

- 1. 클라이언트가 IP 주소를 수신합니다.
- 2. 클라이언트가 브라우저를 열고 웹 사이트에 액세스합니다.
- 3. 클라이언트에서 보낸 첫 번째 TCP 패킷은 WLC에 의해 하이재킹되며, WLC는 Webauth 페이 지를 가로채서 전송합니다.
- 4. DNS가 올바르게 구성된 경우 클라이언트는 Webauth 페이지를 가져옵니다.
- 5. 인증하려면 클라이언트가 사용자 이름/비밀번호를 제공해야 합니다.
- 6. 인증에 성공하면 클라이언트가 원래 액세스 페이지로 리디렉션됩니다.

Welcome to the Cisco wireless network Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work. User Name Password	Login		
Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.	Welcome to	the Cisco wireless network	
User Name Password	Cisco is please your network. Pl solution to work	d to provide the Wireless LAN infrastructure for ease login and put your unified wireless	
Password	User Name		
	obor nume		

7. 클라이언트가 올바른 자격 증명을 제공하면 클라이언트가 인증을 전달합니다.

Ð	Artp://www.google.com/	Internet Explorer cannot dis ×	
	⊘ Logout - Windows Internet Explorer □ □ ⊘ https://192.168.200.1/lc S Certi	vebpage	
	Web Authentication		
	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:		
	https://192.168.200.1/logout.html Logout		



컨피그레이션의 문제를 해결하려면 게스트 앵커 역할을 하는 5508 Series WLC에 다음 디버그를 입력합니다.

Debug Client

Debug web-auth redirect enable mac

예를 들면 다음과 같습니다.

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 00:00:00:00:00:00(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 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

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: fe80:0000:0000:6c1a: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 guest 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 TPv4 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 -60.60.60.251 (local address 60.60.60.2, 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 transmitting DHCP REQUEST (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

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

다음은 클라이언트 측 패킷 캡처입니다.

클라이언트가 IP 주소를 가져옵니다.

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
Contraction and the second second		and the second sec	An an Andreas and a destance of the second discovery and

```
클라이언트가 브라우저를 열고 www.facebook.com을 입력합니다.
```

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 0xab1b 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 Oxabib _ AAAA_www.facebook.com	
•				
■ Frame 508: 76	bytes on wire (608 bit	ts), 76 bytes captured (608	bits) on interface 0	
🗉 Ethernet II. S	rc: Smartlin_2f:b6:9a	(00:17:7c:2f:b6:9a), Dst:	Cisco_fc:96:a8 (f0:f7:55:fc:96:a8)	
Internet Proto	col version 4, Src: 60	0.60.60.11 (60.60.60.11), D	st; 50,50,50,251 (50,50,50,251)	
User Datagram	Protocol, Src Port: 62	2672 (62672), Dst Port: dom	ain (53)	
Domain Name Sy	stem (query)			
Transaction	ID: 0xab1b			
■ Flags: 0x0100 Standard query				
Questions: 1				
Answer RRs: 0				
Authority RRs: 0				
Additional RRs: 0				
Oueries				
www.facebook.com: type AAAA, class IN				

WLC는 클라이언트의 첫 번째 TCP 패킷을 가로채고 가상 IP 주소 및 내부 Webauth 페이지를 푸시 합니다.

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://doi.org/10.1011/001100000000000000000000000000
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: Smartlin_2f:b6:9a (00:17:7c:2f:b6:9a)
 Internet Protocol Version 4, Src: 56.56.56.56 (56.56.56), Dst: 60.60.60.11 (60.60.60.11)
 Transmission Control Protocol, Src Port: http (80), Dst Port: 49720 (49720), Seq: 1, Ack: 207, Len: 470
- Hypertext Transfer Protocol Hypertext Transfer Protocol HTP/1.1 200 oK\r\n Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico\r\n Content-Type: text/html\r\n

. .

- Content-Length: 323\r\n
- \r\n
- [HTTP response 1/1]

웹 인증에 성공하면 나머지 워크플로가 완료됩니다.

60.60.60.11	50.50.50.251	DNS	86 Standard query 0x64dd A ie9cvlist.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 > 49724 [ACK] seq=1 Ack=137 win=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] seg=139 Ack=196 win=6656 Len=0
40 40 40 11	40 40 40 315	A PRIME	AT HERE WHEN HE TOTAL AR

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.