ةكبشلا يف مكحتلا تادحو فيض ءاسرا دحوملا لوصولل ةيكلساللا (LAN) ةيلحملاً عمجملاً لوصولاً نيوكت لاثم عم

المحتويات

<u>المتطلبات الأساسية</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>التكوين</u> <u>الرسم التخطيطي للشبكة</u> <u>الجزء 1 - التكوين على عنصر التحكم WLC 5508 الخاص بالارتباط</u> <u>الجزء 2 -تكوين إمكانية التنقل للوصول المجمع بين السلسلة 5760/5508 من WLC ومحول Catalyst 3850 Series Switch الجزء 3: التكوين على المحول Assist Series Switch والمحمع الارتباط التحقيق من الصحة <u>التحقق من الصحة</u></u>

المقدمة

يصف هذا وثيقة كيف أن يشكل ال sery 5760/5508 لاسلكي lan جهاز تحكم (WLCs) والمادة حفازة sery 3850 مفتاح ل ال wireless زبون إثرزة في الجديد حركية توزيع عملية إعداد حيث ال wireless (بط sery WLC 5508 يعمل كالحركة ربط والمادة حفازة sery 3850 مفتاح يعمل كحركية جهاز تحكم خارجي للعملاء. بالإضافة إلى ذلك، المادة حفازة 3850 sery sery يعمل مفتاح كعميل تنقل إلى sery WLC 5760 أن يعمل كجهاز تحكم حركي من حيث المادة حفازة 3850 sery يحصل مفتاح على ترخيص نقطة الوصول (ap).

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من هذا موضوع قبل أن يحاول أنت هذا تشكيل:

- Cisco IOS[®] GUI أو CLI مع Converged Access 5760 و sery WLCs 3650 ومادة حفازة sery 3850 evi مفتاح
 - الوصول إلى واجهة المستخدم الرسومية (GUI) وواجهة سطر الأوامر (CLI) مع سلسلة WLC 5508

- تكوين معرف مجموعة الخدمة (SSID)
 - مصادقة الويب

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 5760 الإصدار 3.3.3 (الجيل التالي من خزانة أسلاك [NGWC])
 - محول Catalyst 3850 Series
 - Cisco 5508 Series WLC، الإصدار 7.6.120
- نقاط الوصول في الوضع Lightweight من السلسلة Cisco 3602 Series
 - المحولات Cisco Catalyst 3560 Series Switches

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

تعمل وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5508 كوحدة تحكم إرساء، ويعمل المحول Catalyst 3850 Series switch كوحدة تحكم أجنبية ووكيل التنقل الذي يحصل على الترخيص من وحدة التحكم في التنقل 5760.



ملاحظة: في الرسم التخطيطي للشبكة، تعمل وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5508 كوحدة تحكم في الإرساء، تعمل وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5760 كوحدة تحكم في التنقل، ويعمل المحول Catalyst 3850 Series switch كوكيل التنقل ووحدة تحكم في الشبكة المحلية اللاسلكية (WLC) الخارجية. في أي نقطة زمنية، تكون وحدة التحكم في الإرساء للمحولات من السلسلة Series Switch أو ال Catalyst 3850 هي إما ال 5760 كال التنقل Series WLC من الملسلة العربي أو ال 850 Series أو الحكم في أي نقطة زمنية، تكون وحدة التحكم في الإرساء للمحولات من السلسلة Series WLC أو ال 5760 هي إما ال 5760 Series أو ال 5508

التكوينات

وتتضمن عملية التهيئة ثلاثة أجزاء:

<u>الجزء 1 - التكوين على عنصر التحكم WLC 5508 الخاص بالارتباط</u>

<u>الجزء 2 - تكوين التنقل المجمع للوصول بين Series WLC 5760/5508 والمحولات من السلسلة Catalyst 3850 Series WLC 5760/5508</u> Series Switch

<u> الجزء 3 - التكوين على المحول Foreign Catalyst 3850 Series Switch</u>

الجزء 1 - التكوين على عنصر التحكم WLC 5508 الخاص بالارتباط

1. في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5508، قم بالمرور فوق WLAN > جديد

cisco	MONITOR WLANS CO	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	I 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

المرور عبر **شبكة WLAN > تحرير شبكة WLAN > الأمان > مصادقة الويب الممكنة للطبقة 3** لتكوين أمان 2. الطبقة 3.

WLANs > Edit 'CUWN'
General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers
Layer 3 Security ¹ Web Policy - Passthrough
 Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure¹⁹
Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None Sleeping Client Enable

3. جعل عنوان الربط **محلي** ضمن ال WLAN حركي ربط تشكيل نافذة in order to أضفت ال sery WLC 5508 كالربط. كالربط.

											Sa <u>v</u> e Configural
MONITOR	<u>₩</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	_		-
Mobility A	nchors										
WLAN SSI	D CUM	m									
Switch IP	Address (Anchor)								Data Path	Control Path
local										up	up
Mobility	Anchor Cr	eate									

قم بالمرور فوق **الأمان > WebAuth > صفحة WebAuth** لتكوين صفحة WebAuth المراد إستخدامها ... 4. لمصادقة العميل.

في هذا المثال، يتم تحديد صفحة مصادقة الويب الداخلية ل WLC:

СС

	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	Web Login Page							
 AAA General RADIUS Authentication Accounting Fallback Date 	Web Authentication Redirect URL after In This page allows you tr page. The Login page i WLAN if 'Web Authentin	Type ogin o customize the co s presented to wel cation" is turned or	Inter Inter Intert and appe b users the firs In (under WLAN	mal (Default) earance of the t time they act Security Polici	Login cess the es).	•]
DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	DNS TACACS+ Cisco Logo LDAP Headline Local Net Users Message MAC Filtering Disabled Clients User Login Policies AP Policies		w CHide					

5. إنشاء مستخدم صاف محلي. يتم إستخدام زوج اسم المستخدم/كلمة المرور هذا من قبل المستخدم عند مطالبته على صفحة WebAuth.

cisco	MONITOR <u>W</u> LANS		WIRELESS	SECURITY	MANAGEMENT	(
Security	Local Net Users	> Edit				
▼ AAA General ▼ RADIUS	User Name Password	surbg				
Authentication Accounting Fallback	Confirm Password Creation Time	••• Mon N	lay 19 12:00:4	1 2014		
► TACACS+ LDAP Local Net Users	Remaining Time WLAN Profile Description		N/A Any WLAN 🔻 surbg			
MAC Filtering						

الجزء 2 -تكوين إمكانية التنقل للوصول المجمع بين السلسلة WLC 5760/5508 من WLC ومحول Catalyst 3850 Series Switch

في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5508، أضف عنصر التحكم في الشبكة 1. المحلية اللاسلكية (WLC) من السلسلة 5760 كنظير التنقل.

းပြားပြား cisco	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	неца (EEEOBACK	_	_	\$
Controller	Static Mobility Group	Members								
General Inventory	Local Nobility Group	Mobile-1								
Interfaces	NAC Address	IP Address		Public	IP Address	Group N	Same	Multicast IP		Status
Interface Groups	58:8d:09:cd:ac:60	10.105.135.151		10.105	135.151	Mobile-1		0.0.0.0		Up
Multicast										
Network Routes	00:00:00:00:00:00	10.105.135.178		10.105	.135.178	surbg		0.0.0		Up
Eedundancy	00:00:00:00:00:00	10.105.135.244		10.105	135.244	surbg		0.0.0.0		Up
Internal DHCP Server										
 Mobility Management Mobility Configuration Mobility Groups 										

في وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5760، تعمل كوحدة تحكم في التنقل، 2. فقم بإضافة وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5508 كنظير التنقل.

ahah							
CISCO Wireless Controller		🛆 Home	Monitor • Configuration	Administration •	Help		
Controller	Mot	ailty Peer					
* 🧰 System	Ne	H Remove					
General		IP Address	Public IP Address	Group Name	Multicast IP	Control Link Status	Data Link Status
Multicast		10.105.135.244	-	gdfue	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	gdfue	0.0.0.0	UP	UP
Internal DHCP Server							
Management							
* 🔁 Mobility Management							
Mobility Global Config							
Mobility Peer							
Switch Peer Group							

هذه الخطوة مهمة جدا! إضافة المحول Catalyst 3850 Series Switch كعميل Mobility على وحدة التحك**β**. في الشبكة المحلية اللاسلكية (WLC) من السلسلة 5760 ضمن علامة التبويب Switch Peer Group تحت إدارة التنقل.

cisco Wireless Controller				
	Ω Home Mor	nitor V Configuration V Ad	Iministration I 💌 Help	
Controller	Switch Peer Group > SURBG-S Switch Peer Group > SURBG-SPG	PG .		
* 💼 System				
Ceneral	New Remove			
Multicast	IP Address	Public IP Address	Control Link Status	Data Link Status
Interfaces	0 10.105.135.226	10.105.135.226	<mark>. OP</mark>	UP
VLAN				
Internal DHCP Server				
🕨 🧰 Management				
🕶 🚍 Mobility Management				
Mobility Global Config				
Mobility Peer				
Switch Peer Group				

على المادة حفازة sery 3850 مفتاح، أضفت ال sery WLC 5760 بما أن الحركة جهاز تحكم. ما إن يتم أنت4. هذا، المادة حفازة sery 3850 مفتاح يمسك ال AP ربط ترخيص من ال حركية جهاز تحكم 5760.

ahaha				
cisco Wireless Controller	🟡 Home	Monitor 🔻	Configuration 🔻	Administration
Controller	Mobility Agent Configurat	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	ime <mark>-</mark>	SURBG-SPG	
🕶 🗁 Mobility Management	DTLS Mode		Enabled	
Mobility Global Config	Mobility Domain ID for 802.11	r	0xe699	
Mobility Peer	Mobility Keepalive Interval (1-	30)sec	10	

الجزء 3: التكوين على المحول Foreign Catalyst 3850 Series Switch

المرور فوق **واجهة المستخدم الرسومية (GUI) > التكوين > لاسلكي > WLAN > جديد** لتكوين SID/WLAN**.** الدقيق على المحول Catalyst 3850 Series Switch.

alado			
cisco wireless controller	🏠 Home	Monitor V Configuration V Administration V Help	
Wireless	WLAN WLAN > Edit		
* 😂 WLAN	General Security	QOS AVC Policy Mapping Advanced	
WLANS			
Access Points	Profile Name	CUWN	
802.11a/n/ac	Туре	WLAN	
802.11b/g/n	SSID	CUWN	
Media Stream	Status	Enabled	
* <mark>=</mark> QOS	Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	- IA	
	Interface/Interface Group(G	3) VLAN0060 P	
	Broadcast SSID		
	Multicast VLAN Feature		

المرور عبر **شبكة WLAN > تحرير شبكة WLAN > الأمان > مصادقة الويب الممكنة للطبقة 3** لتكوين أمان 2. الطبقة 3.

cisco Wireless Controller	Administration I ▼ Administration I ▼ Help
Wireless WLAN WLANs Access Points B02.11a/n/ac B02.11b/g/n Media Stream QOS	WLAN WLAN > Edit General Security QOS AVC Policy Mapping Advanced Layer2 Layer3 AAA Server Web Policy V Conditional Web Redirect V Webauth Authentication List Disabled V Webauth Parameter Map Web V Webauth On-mac-filter Failure Preauthentication IPv4 ACL Unconfigured
	Preauthentication IPv6 ACL

3. أضفت ال sery WLC 5508 عنوان بما أن الربط تحت ال WLAN حركية ربط تشكيل

altalia cisco Wireless Controller	Administration ▼ Help
Wireless	Mobility Anchors WLAN > Edit
WLAN WLAN Access Points	WLAN Profile QUWN
▶ 🧰 802.11a/n/ac ▶ 🧰 802.11b/g/n	Create Mobility Anchor
 Media Stream QOS 	IP Address ID 10.105.135.151

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

توصيل العميل بشبكة WLAN Cisco اللاسلكية الموحدة (CUWN). فيما يلي تدفق العمل:

- 1. يستلم العميل عنوان IP.
- 2. يفتح العميل متصفح ويدخل أي موقع ويب.
- 3. يتم إختطاف حزمة TCP الأولى التي يرسلها العميل بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، ويعترض عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ويرسل صفحة WebAuth.
 - 4. إذا تم تكوين DNS بشكل صحيح، يحصل العميل على صفحة WebAuth.
 - 5. يجب أن يوفر العميل اسم المستخدم/كلمة المرور للمصادقة. بعد إجراء مصادقة ناجحة، تتم إعادة توجيه العميل إلى صفحة الوصول الأصلية.

Login 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	Attps://19	92.168.200.1 🔎 – 😵 C. 🗟 🖒 🗙 <i>i</i> Web Authentication	×
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.	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	Cisco is pleased your network. Ple solution to work.	to provide the Wireless LAN infrastructure for ase login and put your unified wireless	
	User Name		
Password	Password		

7. بعد أن يوفر العميل بيانات الاعتماد الصحيحة، يقوم العميل بتمرير المصادقة.

4	\bigcirc // http://www.google.com/ $\rho \neq c \times$	Internet Explorer cannot dis X
	Cogout - Windows Internet Explorer	
	🥃 https://192.168.200.1/lc 😵 Certi 🗟 🏠 🏠	👸 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	
	€ 100% ▼	

استكشاف الأخطاء وإصلاحها

دخلت in order to تحريت تشكيلك، هذا يضبط على ال sery WLC 5508، أي يعمل كضيف ربط:

Debug Client

Debug web-auth redirect enable mac

فيما يلي مثال:

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 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* (0)00:00:00:00:00:00

(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* to 255 255 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: fe80:0000:0000:6c1a: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 00:00:00:00:00:00, 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* (local address 60.60.60.2, gateway 60.60.60.251, VLAN 60, port 1) 60.60.60.251 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* secs: 3072, flags: 0 ,(2902502819) :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* (len 358, port 1, vlan 60) 60.60.60.251 - 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* (len 308, vlan 60, port 1, encap 0xec00) (2) 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* secs: 0, flags: 0 ,(2902502819) :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* rcvd server id: 60.60.60.251 192.168.200.1 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

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* (Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8 (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* (Change state to RUN (20) last state WEBAUTH_NOL3SEC (14 (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 éaol alog alog alog.

يحصل العميل على عنوان 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? τell 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
E-BALLER - Later - Jack	6600	The second se	Complete and identical framework Management and

يفتح العميل متصفح ويصنف www.facebook.com.

			at talke a neep prenty and ear they take with over a set		
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 Oxabib _ AAAA_www.facebook.com		
•					
Frame 508: 76	bytes on wire (608 bi	ts), 76 bytes captured (608 b	bits) on interface O		
🗉 Ethernet II,	Src: Smartlin_2f:b6:9a	(00:17:7c:2f:b6:9a), Dst: Cf	isco_fc:96:a8 (f0:f7:55:fc:96:a8)		
Internet Prot	ocol version 4, Src: 6	0.60.60.11 (60.60.60.11), Dst	t: 50.50.50.251 (50.50.50.251)		
🗉 User Datagram	B User Datagram Protocol, Src Port: 62672 (62672), Dst Port: domain (53)				
Domain Name S	□ Domain Name System (query)				
Transaction ID: Oxablb					
🗃 Flags: 0x0100 Standard query					
Questions: 1					
Answer RRs: 0					
Authority RRs: 0					
Additional RRs: 0					
🖶 Queries					
⊞ www.facebook.com: type AAAA, class IN					

يعترض عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) حزمة TCP الأولى للعميل ويدفع عنوان IP الظاهري الخاص به وصفحة WebAuth الداخلية.

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/10.1011/001010000000000000000000000000

- 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 ■ HYPERTEXT Transfer Protocol ■ HTTP/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-input: text/html\r\n

 Content-Length: 323\r\n \r\n

[HTTP response 1/1] . .

بعد مصادقة الويب الناجحة، يتم إكمال باقي سير العمل.

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 w1n=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 PROVINCE	DO NAME AND TO TOTAL OC.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما