Gastanker voor Unified Access Wireless LANcontrollers met configuratievoorbeeld voor geconvergeerde toegang

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram Configuraties Deel 1 - Configuratie op de 5508 Anker WLC Deel 2 - Configuratie van geconvergeerde toegangsmobiliteit tussen de 5508/5760 Series WLC en Catalyst 3850 Series Switch Deel 3: Configuratie op de Foreign Catalyst 3850 Series Switch Verifiëren Problemen oplossen

Inleiding

In deze documenten wordt beschreven hoe de 5508/5760 Series draadloze LAN-controllers (WLC's) en de Catalyst 3850 Series Switch voor de draadloze client moeten worden geconfigureerd als Gastanker in de nieuwe installatie voor mobiliteitsplanning waarbij de 5508 Series WLC fungeert als het Mobility Anker en de Catalyst 3850 Series Switch fungeert als een Mobility Foreign Controller voor de clients. Bovendien fungeert de Catalyst 3850 Series Switch als een Mobility Agent voor een 5760 Series WLC die fungeert als een Mobility Controller van waaruit de Catalyst 3850 Series Switch de Access Point (AP)-licentie verkrijgt.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen voordat u deze configuratie probeert:

• Cisco IOS[®] GUI of CLI met de geconvergeerde access 5760 en 3650 Series WLC's en de

Catalyst 3850 Series Switch

- GUI- en CLI-toegang met de 5508 Series WLC
- Configuratie van Service Set Identifier (SSID)
- Web verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5760 release 3.3.3 (kabelkasten van de volgende generatie [NGWC])
- Catalyst 3850 Series Switch
- Cisco 5508 Series WLC-release 7.6.120
- Cisco 3602 Series lichtgewicht access points
- Cisco Catalyst 3560 Series switches

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Opmerking: Gebruik de <u>Command Lookup Tool</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

De 5508 Series WLC fungeert als een ankercontroller en de Catalyst 3850 Series Switch fungeert als een buitenlandse controller en de Mobility Agent die de licentie verkrijgt van de Mobility Controller 5760.



Opmerking: in het netwerkdiagram fungeert de 5508 Series WLC als de ankercontroller, de 5760 Series WLC fungeert als de Mobility Controller en de Catalyst 3850 Series Switch fungeert als de Mobility Agent en Foreign WLC. Op elk moment is de ankercontroller voor de Catalyst 3850 Series Switch de 5760 Series WLC of de 5508 Series WLC. Beide kunnen geen ankers tegelijkertijd zijn, omdat het dubbele anker niet werkt.

Configuraties

De configuratie bestaat uit drie delen:

Deel 1 - Configuratie op de 5508 Anker WLC

Deel 2 - Configuratie van geconvergeerde toegangsmobiliteit tussen de 5508/5760 Series WLC en Catalyst 3850 Series Switch

Deel 3 - Configuratie op de Foreign Catalyst 3850 Series Switch

Deel 1 - Configuratie op de 5508 Anker WLC

1. Op de 5508 Series WLC, hang over **WLAN > Nieuw** om een nieuw draadloos LAN (WLAN) te maken.

cisco	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit 'CUW	N'
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	I Enabled
	NAS-ID	5508

2. Beweeg via WLAN > WLAN Edit > Security > Layer 3-enabled webverificatie om Layer 3 Security te configureren.

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 ¹ 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. Maak het Ankeradres **lokaal** onder het WLAN-mobiliteitsankerconfiguratievenster om de 5508 Series WLC als anker toe te voegen.

										Sa <u>v</u> e Configural
MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK		
Mobility A	Inchors									
WLAN SSI	D CUN	N								
Switch IP	Address (Anchor)							Data Path	Control Path
local									up	up
an - Lubra										

4. Ga naar **Security > Webauth > Webauth pagina** om de Webauth-pagina te configureren die gebruikt moet worden voor de clientverificatie.

In dit voorbeeld, wordt de WLC Interne Webauth pagina geselecteerd:

ດໄທໄທ cisco		WLANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	Web Log	n Page							
AAA General RADIUS Authentication Accounting Fallback Due	Web Auth Redirect U This page all page. The Lo WLAN if 'Web	entication JRL after lo lows you to ogin page is b Authentic	Type gin customize the col presented to wet ation' is turned on	Inter Intert and appe o users the first (under WLAN	mal (Default) arance of the l t time they acc Security Policie	Login ress the es).	•]
TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Cisco Log Headline Message	0	© Sho	w ©Hide					

5. Maak een lokale netwerkgebruiker. Dit gebruikersnaam/wachtwoord-paar wordt door de gebruiker gebruikt wanneer dit op de Webauth-pagina wordt gevraagd.

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

Deel 2 - Configuratie van geconvergeerde toegangsmobiliteit tussen de 5508/5760 Series WLC en Catalyst 3850 Series Switch

1. Op de 5508 Series WLC, voeg de 5760 Series WLC toe als de Mobility Peer.

cisco	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEOBACK	_	_	s
Controller	Static Mobility Group	Members								
General Inventory	Local Nobility Group	Mobile-1								
Interfaces	MAC Address	IP Address		Public	IP Address	Group	Name	Nulticast IP	Sta	stus
Interface Groups	58:8d:09:cd:ac:60	10.105.135.151		10.105	135.151	Mobile	-1	0.0.0.0	Up	
Multicast	00:00:00:00:00:00	10.105.135.170		10.105	.135.178	surbg		0.0.0.0	Up	
 Redundancy 	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 										

2. Op de 5760 Series WLC, die als een Mobility Controller optreedt, voeg de 5508 Series WLC toe als de Mobility Peer.

-titulta cisco Wireless Controller	🛆 Hom	e Monitor 💌 Configuratio	an 🔹 Administration I 🕶	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		subg	0.0.0.0		-
Interfaces	10.105.135.151	10.105.135.151	Mobie-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						

3. Deze stap is heel belangrijk! Voeg de Catalyst 3850 Series Switch toe als Mobility Agent op de 5760 Series WLC onder het tabblad Switch Peer Group onder Mobility Management.

cisco Wireless Controller	A Home Manitor	Confouration Administra	ation V 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. Op de Catalyst 3850 Series Switch, voeg de 5760 Series WLC toe als de Mobility Controller. Zodra u dit doet, de Catalyst 3850 Series Switch grijpt de AP kan licentie van de Mobility Controller 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

Deel 3: Configuratie op de Foreign Catalyst 3850 Series Switch

1. Beweeg de muis over **GUI > Configuration > Wireless > WLAN > Nieuw** om de exacte SSID/WLAN op de Catalyst 3850 Series Switch te configureren.

ahaha		
cisco Wireless Controller	🟦 Home	Monitor Configuration Administration Help
Wireless	WLAN	
	WLAN > Edit	
* 📴 WLAN	General Security	QOS AVC Policy Mapping Advanced
WLANS		
Access Points	Profile Name	COWN
802.11a/n/ac	Туре	WLAN
902.11b/g/n	SSID	CUWN
Media Stream	Status	✓ Enabled
QOS		Web-auth
	Security Policies	(Modifications done under security tab valiancear after archime the changes.)
	Rudio Delev	
	Radio Policy	
	Interface/Interface Group(G)	G) VLANDOGO
	Broadcast SSID	
	Multicast VLAN Feature	

2. Beweeg via WLAN > WLAN Edit > Security > Layer 3-enabled webverificatie om Layer 3 Security te configureren.

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

3. Voeg het WLC IP-adres van 5508 Series toe als anker onder de WLAN-configuratie voor mobiliteitsankers

cisco Wireless Controller	Administration ▼ Help
Wireless	Mobility Anchors WLAN > Edit
WLAN WLAN Access Points B02.11a/n/ac	WLAN Profile CUWN Switch IP Address Create Mobility Anchor
GU2.110/g/n Gu2.110/g/n Gu3 Stream Gu3 QOS	Remove Anchor IP Address 10.105.135.151

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Sluit de client aan op het WLAN Unified Wireless Network (CUWN). Hier is de werkstroom:

- 1. De client ontvangt een IP-adres.
- 2. De client opent een browser en heeft toegang tot elke website.
- 3. Het eerste TCP-pakket dat door de client wordt verzonden, wordt gekaapt door de WLC, en de WLC onderschept en verstuurt de Webauth-pagina.
- 4. Als DNS goed is geconfigureerd, krijgt de client de Webauth-pagina.
- 5. De client moet de gebruikersnaam/het wachtwoord opgeven om te worden geverifieerd.
- 6. Na succesvolle verificatie wordt de client omgeleid naar de oorspronkelijke toegangspagina.

	192.168.200.1 $ P$ 🗸 😵 C. 🗟 C 🗙 🏈 Web Authentication	×
Login		
Welcome to	the Cisco wireless network	
Cisco is please your network. Pl solution to work	d to provide the Wireless LAN infrastructure for ease login and put your unified wireless	
User Name		
Password		

7. Nadat de client de juiste referenties heeft opgegeven, gaat de client over op de auth.

æ		<i>i</i> Internet Explorer cannot dis ×
Ş	Cogout - Windows Internet Explorer Definition (Content of the second sec	x 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: https://192.168.200.1/logout.html	
	€ <mark>100%</mark>	

Problemen oplossen

Om uw configuratie problemen op te lossen, voer deze debugs in op de 5508 Series WLC, die fungeert als Gastanker:

Debug Client

Debug web-auth redirect enable mac

Hierna volgt een voorbeeld:

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)

*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: fe80:0000:0000:6c1a: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, slot 0, interface = 1, QOS = 0 IPv4 ACL ID = 255, IPv6 ACL ID =

Hier is de client-side pakketopname.

De client krijgt het IP-adres.

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
C. BALLER A. LARS		and the second sec	An an Indexes a destance for each the second of

De client opent een browser en typt www.facebook.com.

			a state a state franci weathers that the state and the state			
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 0xab1b AAAA www.facebook.com			
60.60.60.11	50, 50, 50, 251	DNS	76 Standard query Oxabib _ AAAA_www.facebook.com			
•						
Frame 508: 76	oytes on wire (608	bits), 76 bytes captured (608 b	oits) on interface O			
🗉 Ethernet II, Sr	<pre>rc: Smartlin_2f:b6:</pre>	9a (00:17:7c:2f:b6:9a), Dst: Ci	sco_fc:96:a8 (f0:f7:55:fc:96:a8)			
Internet Proto	Internet Protocol Version 4, Src: 60.60.60.11 (60.60.60.11), Dst: 50.50.50.251 (50.50.50.251)					
B User Datagram Protocol, Src Port: 62672 (62672), Dst Port: domain (53)						
□ Domain Name System (query)						
Transaction 1	Transaction ID: Oxablb					
Flags: 0x0100	🗄 Flags: 0x0100 Standard query					
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
🖶 Queries						
🖩 www.facebook.com: type AAAA, class IN						

De WLC onderschept het eerste TCP-pakket van de client en drukt op het virtuele IP-adres en de interne Webauth-pagina.

56	. 56. 56. 56	60.60.60.11	TCP	54 http > 49720	[ACK] Seq=1 A	ck=207 win=6656 L	.en=0
56	. 56. 56. 56	60.60.60.11	HTTP	524 HTTP/1.1 200	OK (text/htm	1)	
56	56 56 56	60 60 60 11	TCP	54 http://www.sec.54	FETN ACK' SP	n=471 Ark=207 wir	=6656 LAN=0
4							
۲	Frame 550: 524 by	tes on wire (4192 bits), 524 by	tes captured (4	192 bits) on inte	rface 0		
÷	Ethernet II, Src	: C1sco_TC:96:a8 (T0:T7:55:TC:94	s:a8), Dst: smar	tlin_27:66:9a (00	:17:7C:2T:D6:	9a)	
۲	Internet Protoco	l Version 4, Src: 56.56.56.56 (i6.56.56.56), Ds	t: 60.60.60.11 (6	0.60.60.11)		
	Transmission Cont	rol Protocol, Src Port: http (8	0), Dst Port: 4	9720 (49720), Seq	: 1, Ack: 207	, Len: 470	
	B Hypertext Transfer Protocol						
	E HTTP/1.1 200 0€	(\r\n					
	Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico\r\n						
	Content-Type: 1	text/html\r\n					
	Content-Length:	: 323\r\n					
	\r\n						
	[HTTP response	1/1]					

Na succesvolle webverificatie wordt de rest van de werkstroom voltooid.

60.60.60.11	50.50.50.251	DNS	86 Standard query Dx64dd 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 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 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 31	40 40 40 315	ALCONOM.	DO NAME AVERAGE NO TEXTADOOD

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.