Wired Guest Access using Cisco WLAN Controllers Configuration Example

Contents

Introduction Prerequisites Requirements Components Used Configure Access Layer Switch Configuration Important Points for Wired Guest Deployment Platform Support Wireless LAN Configuration Wired Guest Access with Anchor WLAN Controller Wired Guest Client Configuration Debugs for Wired Guest Connection on Local WLC Verify Troubleshoot Related Information

Introduction

This document describes how to configure guest access with the new Wired Guest Access feature support on the Cisco WLAN Controllers (WLCs) that use Cisco Unified Wireless Software Release 4.2.61.0 and later. A growing number of companies recognize the need to provide Internet access to its customers, partners, and consultants when they visit their facilities. IT managers can provide wired and wireless secured and controlled access to the Internet for guests on the same wireless LAN controller.

Guest users must be allowed to connect to designated Ethernet ports and access the guest network as configured by the administrator after they complete the configured authentication methods. Wireless guest users can easily connect to the WLAN Controllers with the current guest access features. In addition, Wireless Control System (WCS), along with basic configuration and management of WLAN Controllers, provides enhanced guest user services. For customers who have already deployed or plan to deploy WLAN Controllers and WCS in their network, they can leverage the same infrastructure for wired guest access. This provides a unified wireless and wired guest access experience to the end users.

Wired guest ports are provided in a designated location and plugged into an access switch. The configuration on the access switch puts these ports in one of the wired guest Layer 2 VLANs. Two separate solutions are available to the customers:

• A single WLAN controller (VLAN Translation mode) - the access switch trunks the wired guest traffic in the guest VLAN to the WLAN controller that provides the wired guest access solution. This controller carries out the VLAN translation from the ingress wired guest VLAN to the

egress VLAN.

• Two WLAN controllers (Auto Anchor mode) - the access switch trunks the wired guest traffic to a local WLAN controller (the controller nearest to the access switch). This local WLAN controller anchors the client onto a Demilitarized Zone (DMZ) Anchor WLAN controller that is configured for wired and wireless guest access. After a successful handoff of the client to the DMZ anchor controller, the DHCP IP address assignment, authentication of the client, and so on are handled in the DMZ WLC. After it completes the authentication, the client is allowed to send/receive

traffic.



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The Wired Guest Access feature support on the Cisco WLAN controllers is supported by Cisco Unified Wireless Software Release 4.2.61.0 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

In this section, you are presented with the information to configure the features described in this document.

Access Layer Switch Configuration

In order to provide the wired guest access, the designated ports in the Layer 2 access layer switch need to be configured on the guest VLAN by the administrator. The guest VLAN must be separate from any other VLANs that are configured on this switch. The guest VLAN traffic is trunked to the nearest WLAN local controller. The local controller tunnels the guest traffic across an Ethernet over IP (EoIP) tunnel to a DMZ Anchor controller. This solution requires at least two controllers.

Alternatively, the access switch trunks the guest VLAN to the single controller translates the guest VLAN to the egress interface of the WLAN controller.

cat6506# show vlan id 49 VLAN Name Status Ports _____ _____ active Gi2/1, Gi2/2, Gi2/4, Gi2/35 VLAN0049 49 Gi2/39, Fa4/24 VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 enet 100049 1500 - -_ _ _ 0 0 49 Remote SPAN VLAN _____ Disabled Primary Secondary Type Ports _____ ____ cat6506# interface FastEthernet4/24 description Wired Guest Access switchport switchport access vlan 49 no ip address end cat6506# interface GigabitEthernet2/4 description Trunk port to the WLC switchport switchport trunk native vlan 80 switchport trunk allowed vlan 49,80,110 switchport mode trunk no ip address end

Note: Use the <u>Command Lookup Tool</u> (<u>registered</u> customers only) to find more information on the commands used in this document.

Important Points for Wired Guest Deployment

- Currently, five Guest LANs for wired guest access are supported. In total, 16 WLANs for Wireless users and 5 WLANs for wired guest access can be configured on the Anchor WLC. No separate tunnels exist for WLANs. All the guest WLANs, which include the WLANs for wired guest access, use the same EoIP tunnels to the Anchor WLC.
- Administrators need to create dynamic interfaces in the WLAN controller, mark them as "Guest LAN," and associate them to WLANs created as Guest LANs.
- Ensure that WLAN configurations, including authentication, are identical on both the Anchor and Remote controllers to pass the client traffic.
- WLCs should have compatible software versions. Ensure that they run the same major version.
- Web-authentication is the default security mechanism available on a wired guest LAN. The current options available are these: Open, Web Auth, and Web Passthrough.
- In case of failure of the EoIP tunnel between the remote and anchor WLC, the client database is cleaned up from the Anchor WLC. The client needs to reassociate and reauthenticate.
- No Layer 2 security is supported.
- Multicast/Broadcast traffic on the wired guest LANs is dropped.
- DHCP Proxy settings must be identical on both the Anchor and Remote controllers.

For the wired guest, there is an idle timeout that runs in the controller. If no packets are received within the configured period from the client, the client is removed from the controller. When a client sends an Address Resolution Protocol (ARP) request the next time, a new client entry is created and moved to the Web Auth/run state appropriately as per the security configuration.

Platform Support

Wired guest access is supported on these platforms:

• Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM2, Virtual WLC

Wireless LAN Configuration

In this example, the basic configuration of the wireless LAN controller is assumed. The focus is on the additional configuration required to complete the wired guest access implementation.

 Create a dynamic interface and mark it is as a "Guest LAN." When you create this dynamic interface in the current release, you need to provide an IP address and default gateway, even though it does not exist since it is a Layer 2 VLAN; you need not provide any DHCP address. Wired guest clients are physically connected to this VLAN.

cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Interface	s > Edit						
General Inventory	General I	nformatio	on					
Interfaces	Interface	Name	wired-vl					
Multicast	MAC Add	lress	00:18:b					
Internal DHCP Server	Interface	Address						
Mobility Management	VLAN Ide	ntifier	49					
Ports	IP Addres	55	10.10	.49.2				
NTP	Netmask		255.2	55.255.0				
CDP	Gateway		10.10	.49.1				
P Advanced	Physical I	Informati	on					
	Port Num	ber	1					
	Backup P	ort	0					
	Active Po	rt	1					
	Enable D Managerr	ynamic AP hent						
	Configura	tion						
	Quarantir	ne						
	Guest La	n	V					
	DHCP Info	ormation						
	Primary I	DHCP Serve	er 🗌					
	Secondar	ry DHCP Se	rver					
	Access C	ontrol Lis	t					
	ACL Nam	e	none					
	Note: Chang temporarily some clients	ping the Inte disabled an s.	erface parameters of thus may result	causes the WL in loss of conn	ANs to be ectivity for			

2. Create another dynamic interface where the wired guest clients receive an IP address.**Note**: You need to provide an IP address/ default gateway / DHCP server address in this interface.

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP			
Controller	Interface	s > Edit									
General Inventory	General Information										
Interfaces Multicast	Interface MAC Add	Name ress	110 00:18:b								
Network Routes Internal DHCP Server	VLAN Identifier										
Ports NTP	IP Addres	s	10.10	55.255.0							
 CDP Advanced 	Gateway 10.10.110.1										
	Port Num	ber	1								
	Active Po Enable D	ort rt ynamic AP	1								
	Managem Configura	tion									
	Quarantir Guest Lar	ne n									
	DHCP Info	ormation									
	Primary (Secondar	OHCP Serve y DHCP Se	rver	.110.1							
	Access Co	ontrol Lis	t								
	ACL Nam Note: Chang temporarily some clients	e ling the Inte disabled an 1.	none orface parameters d thus may result	causes the WL In loss of conn	ANS to be ectivity for						

3. These are the dynamic interfaces:

interfaces.							
cisco	MONITOR WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT CO	MMANDS HELP	
Controller	Interfaces						
General	Interface Name	VL.	AN Identifier	IP Address	Interface Type	Dynamic AP Manageme	nt
Inventory	110	11	0	10.10.110.2	Dynamic	Disabled	E
Interfaces	ap-manager	un/	tagged	10.10.80.4	Static	Enabled	
Multicast	management	unt	tagged	10.10.80.3	Static	Not Supported	
Network Routes	service-port	N/A	A	0.0.0.0	Static	Not Supported	
Internal DHCP Server	virtual	N/4	A	1.1.1.1	Static	Not Supported	
Mobility Management	wired-vlan-49	49		10.10.49.2	Dynamic	Disabled	
Barts							

4. Add a new WLAN: Type=Guest LAN.

Cisco_48:53:c3 - Microsoft	Internet Explorer			State 3					X BLX
File Edk Vew Pavyrites	Toole Help			222.232					S 🍂
(3 🏠 🔎 Search 😭	Favortes 🧑 🍰	- 2 13	12					Links **
Address Ntps://10.77.244	204/screens/framei.et.html							•	20
ahaha			and the			Saye Co	nfiguration Emp	Logout I	Befresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	1222	1223
WLANs	WLANs > New						< Back	Appl	Y
* WLANS	Туре	Guest LAN	3						
Advanced	Profile Name	Wired-Guest							
	WLAN SSID	Wand-Guest							

5. Enable the WLAN; map the ingress interface to the "Guest LAN" created in Step 1, and the egress interface can be a management interface or any other dynamic interface, although preferably a dynamic interface such as that created in Step

File Edit View Favorites	Tools Help		
👌 tect - 🐑 - 💌	a) 🔥 💭 Search 🔮 Favo	tes 🙆 🔝 🔔 🗔 🗖 📶	Links
Address a https://10.77.244	204/screens/frameset.html		
cisco	MONITOR MUNIC	WTROLLER WIRELESS SECURITY MONA	Sege Configuration Bing Legout Befreit SEMENT COMMANDS HELP
WLANs	WLANs > Edit		< Sack Apply
* WLANS	General Security	QoS Advanced	
Advanced	Profile Name Type SSBD Status Security Policies Ingress Interface Egress Interface	Wind-Currit Guert LAN Wind-Gunit IP Enabled Web-Auth (Modifications done under security tab will appea wired-vian-49 = management =	ar aftar applying the changes.)
	Post Notes 2 Web Policy cannot be o 4 When client exclusion	sed in combination with User of zero means infinity (will require administrative svemide to reset excluded clients)

6. Web authentication is enabled by default as the security option configured on the Guest LAN. It can be changed to *None* or *Web Passthrough*.



7. This is the final configuration of the

WLAN.									
Cisco_48:53x3 - Microsoft Internet Diplorer									
File Edit View Favorites Tools Help									
😋 Bad, + 😥 - 💌 😰 🏠 🔎 Search 👷 Fevorites 🤣 🍰 - 🖕 🥽 🛄 🏭									
Address 👔 https://10.77.244.20	H/screens/frameset.html								
- abala -			Sage Configuration Ping Logout	Lefresh					
CISCO	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP						
WLANs	WLANs.		New						
WEANS			Admin	-					
WLANE	Profile Name	Type WLAN SSID	Status Security Policies						
Advanced	timeb	WLAN tsweb	Enabled [WPA2][Auth(882.1×)]						
	Wired-Guest	Guest LAN Wired-Guest	Enabled Web-Auth	-					

8. Add a guest user in the local database of the WLC.

File Edt View Favorites	Tools Help					4
🌀 Back + 🎲 - 💌 💈	. 🏠 🔎 Search 🤺 Favori	= 🚱 🝰 😓 🗔 📒	111			Links
kddress 👔 Https://10.77.244.20	4/screens/frameset.html					. 🔁 🖸 👀
cisco	MONITOR WLANS CO	NTROLLER WIRELESS SEC	URITY MANAGEN	Saxe Co MENT C <u>O</u> MMANDS	nfiguration Eing HELP	Logout Befresh
Security • ARA General • RADIUS Authentication Accounting Fallback • TACACS+ LDAP LOAD AP ADICIES POICIES POICIES POICIES	Local NetUsers > Edi User Name Password Confirm Password Lifetime (seconds) Guest User Role Creation Time Remaining Time WLAN Profile Description	t guest 96400 Thu Nov 20 14:12:32 2000 23 h 59 m 56 s Wired-Guest (m) Wired-guest			< Back	Apply
Done	-			1	🐴 🙂 21	ternet

On the Foreign, you need to set the ingress as the configured "Guest LAN." At the egress, you need to set it to some interface, possibly the management interface. However, once the EoIP tunnel is built, it sends the traffic automatically through the tunnel instead of the management address.

Wired Guest Access with Anchor WLAN Controller

In this example, the IP address of the remote wireless LAN controller is 10.10.80.3, and the IP address of the Anchor DMZ controller is 10.10.75.2. Both are part of two different mobility groups.

 Configure the mobility group of the Anchor DMZ controller when you add the MAC address, IP address, and mobility group name of the remote controller.

and a hadron of the second								
cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller General Inventory Interfaces Multicast Network Routes Internal DHCP Server Mobility Management Mobility Groups	Mobility C This page al Mobility ground mobility ground address and spaces. 00:10:73:3 00:18:b9:0	WLANS Group Me lows you to up member up member i group nam 14:b2:60 ea: a7:20	controller embers > Edit o edit all mobility ; s are listed below is represented as ne(optional) separ 10.10.75.2 10.10.80.3 to	All group members , one per line. E s a MAC addres ated by one or i	SECURITY at once. Each iss, IP more	MANAGEMENT	COMMANDS	HELP
Mobility Anchor Config Ports NTP CDP Advanced					Ŧ			

2. Similarly, configure the mobility group in the remote

control	ler
CONTINUE	101.

cisco	MONITOR	WII ANIE			SECURITY	MANAGEMENT	COMMANDS	
Controller	Mabiliby	Stoup M		All	2000011	-Breachen	0 <u>0</u> mmH100	LICT.
General Inventory Interfaces Multicast	This page al Mobility grou mobility grou address and spaces.	lows you to up member up member I group nam	o edit all mobility s are listed below is represented as ne(optional) separ	group members r, one per line. E s a MAC addres ated by one or r	at once. Each ss, IP more			
Network Routes	00:18:b9:4 00:18:73:3	ea:a7:20 34:b2:60	10.10.80.3 10.10.75.2 mo	bile-9	*			
Mobility Management Mobility Groups Mobility Anchor Config								
Ports					-1			
NTP					12.0			
 CDP Advanced 								

3. Create the wired WLAN with the exact name in the Anchor WLC. The ingress interface in this case is "none" because, logically, the ingress interface is the EoIP tunnel from the remote controller. The egress interface is a different interface, where the wired clients go to receive the IP address. In this example, a dynamic interface called *guest* is created. However, at this stage you cannot enable the WLAN because it displays an error message, which reads that an ingress interface cannot be *none*.



4. Configure Layer 3 security as *web authentication*, similar to the remote controller.

and talk and		Congress (Service)
CISCO	HORITOR HUME CONTROLLER HIPELESS SECLETS MAINEMENT COMPANIES HEP	
WLANs	<pre>VLANe>Edt</pre>	Apply
* WLANC	General Security Cost Advanced	
WLANK	Lager 2 Lager 3 AAL Services	
* Advanced	Layer 3 becades Preseterization ACL Neone D Overvier Skield Config D Evalle D Eval	

5. Create the mobility anchor on the anchor controller, and map it to itself

1.3011.								
alah								ge Configuration: Ding Logeut Batrick.
CISCO	Bowlow Breve Sol	anouter - eg	euss geoson-	идноснеят сфания	is inth			
WLANs	WLANs							New.
* WLANS	Profile Name	Туре	WLAN SSID	Admin Status	Security Policies			
INLASS	al.	Windless	ф8	Enabled	Web-Auth	•		
* Advanced	<u>a</u> 2	Windless	92	Enabled	Web-Auth			
	al	Windless	q3	Disabled	Web-Auth			
	week.co.td	Wined	wined-paret.	Exobled	Web-Auth	Retries		
						and a		
and the later of t								
CISCO	MONITOR WLANE CON	TROLLER WD	RELESS SECURITY	HERRICEMENT COMMAN	o Hela			
WLANs	Nobility Anchore							< Mack
* WLANS	MLAN SSID wind-p.	the state						
WLAN	South IP Address (Arch	er]				Data Path	Control Path	
* Advenced	local	local			10		Lip	•
	Nability Ambar Cre	ute						
	Switch IP Address (Are	tran)	10.10.00.3					
	Access to Handland Deer		and a second second second					

6. Once the mobility anchor is created, go back and enable the wired WLAN.

cisco	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY N	MANAGEMENT	Saya Co COMMANDS	nfiguration Ping HELP	Cogout Refresh
WLANS WLANS WLANS Advanced	WLANs > Edit General Security Profile Name Type SSID Status	Qo5 Advanced wired-guest-1 Guest LAN wired-guest-1 R Enabled				< Back	Apply
	Security Policies Ingress Interface Egress Interface	Web-Auth (Modifications done unde None 💌 guest 💌	r security tab will	l appear after ap	plying the chang	jes.)	

7. Similarly, create the mobility anchor on the remote WLC for the wired guest WLAN.

LANs	WLANs						New.,
WLANS	Profile Name	Type	WLAN SSID	Admin Status	Security Policies		
NLAS	a1.	Windless	98	Enabled	Web-Auth	•	
	<u>a2</u>	Windless	b 5	Enabled	Web-Auth		
	a1	Windless	q3	Disabled	Web-Auth		
	windshalaned.	wined	wired-guest.	Emobled	Web-Auth	Fachers	
						and a second	
						and the second second	

Choose the IP address of the Anchor WLC and create the mobility anchor.

-iliulii cisco	Romine When Commerces Metrice Stockers Management Commune Hels			ubaxaa (Basi (Bisar) Pue
WLANs	NobElty Anchora			< Back
* WLANS	WLAN SSID Hind-guilt			
> Advanced	Wetch IF Address (Archar)	Data Path	Control Path	
	20.18.79.2	up.	LØ.	
	Publity Anchor Levate			

Check if the data and control path is up. If not, ensure these ports are open between the anchor and remote wireless LAN controller: UDP 16666 or IP 97.

8. Once a wired guest user is connected to the switch and has completed the web authentication, the Policy Manager State must be RUN, and the Mobility Role is Export Foreign.

ahaha			5	age Configuration Ping Logout Refres
CISCO	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY	MANAGEMENT COMM	ANDS HELP
Monitor	Clients > Detail		< Back	Apply Link Test Remove
Summary	Client Properties		AP Properties	
Access Points Statistics	MAC Address	00:0d:60:5e:ca:62	AP Address	Unknown
k con	IP Address	0.0.0.0	AP Name	N/A
k Roman	Client Type	Regular	AP Type	Unknown
Clients	User Name		WLAN Profile	wired-guest-1
Multicast	Port Number	1	Status	Associated
THE COST	Interface	110	Association ID	0
	VLAN ID	110	802.11 Authentication	Open System
	CCX Version	Not Supported	Reason Code	0
	E2E Version	Not Supported	Status Code	0
	Mobility Role	Export Foreign	CF Pollable	Not Implemented
	Mobility Peer IP Address	10.10.75.2	CF Poll Request	Not Implemented
	Policy Manager State	RUN	Short Preamble	Not Implemented
	Mirror Mode	Disable 💌	PBCC	Not Implemented
	Management Frame Protection	No	Channel Agility	Not Implemented
			Timeout	0

Similarly, check for the status in the Anchor WLC. The Policy Manager State must be RUN, and the Mobility Role is Export

Anchor.

				age Configuration Ping Logout Befres
CISCO	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY MANAGEMENT COMM	ANDS HELP
Monitor	Clients > Detail		< Back	Apply Link Test Remove
Summary	Client Properties		AP Properties	
Access Points	MAC Address	00:0d:60:5e:ca:62	AP Address	Unknown
> Statistics	IP Address	10.10.77.11	AP Name	10.10.80.3
> Roques	Client Type	Regular	AP Type	Mobile
Clients	User Name	guest	WLAN Profile	wired-guest-1
Multicast	Port Number	1	Status	Associated
	Interface	guest	Association ID	0
	VLAN ID	77	802.11 Authentication	Open System
	CCX Version	Not Supported	Reason Code	0
	E2E Version	Not Supported	Status Code	0
	Mobility Role	Export Anchor	CF Pollable	Not Implemented
	Mobility Peer IP Address	10.10.80.3	CF Poll Request	Not Implemented
	Policy Manager State	RUN	Short Preamble	Not Implemented
	Mirror Mode	Disable 💌	PBCC	Not Implemented
	Management Frame Protection	No	Channel Agility	Not Implemented
			Timeout	0

Wired Guest Client Configuration

The wired guest client receives an IP address from the egress VLAN but cannot pass any traffic until it completes the web authentication process.

In order to log on as a guest user, follow these steps:

 Open a browser window and enter the desired URL name (for example, www.cisco.com). The guest is redirected to the default webpage of the Wireless LAN controller if web authentication is enabled, and a DNS resolution can be completed for the URL that is entered. Otherwise, enter this URL: https://1.1.1.1/login.html, where the IP address 1.1.1.1 is the virtual IP address of the wireless LAN controller.

Web Authentication	on - Microsoft Internet Explorer		216 X
File Edit View Fav	rantes Taols Help		A 8
G tack + ⊙ +	🖹 🛃 🏠 🔎 Search 👷 Favorites 🤣 🍰 😓 🍇		
Address 🛃 https://1.1.1	1-1/login.html	💌 🄁 Go Linis	° ≨Snagit 🛐 🗹
Google G-	💌 Go 🖟 🧔 👻 🏫 Bookmarks 🕶 🧕 O blocked 🛛 🂝 Check. 💌 🗞 AutoLink. 💌	🗟 AutoFili 🅞 Send to 👻 🔏	🕥 Settings 🕶
Login			
Welcome to t	the Cisco wireless network		
Cisco is pleased for your network.	d to provide the Wireless LAN infrastructure Please login and put your air space to work.		
User Name	guesti		
Password			
	Submit		
		-	2
2 Done		🚔 🄇	Internet

- 2. Enter the username and password that are provided.
- 3. If the login is successful, a browser window notes



Debugs for Wired Guest Connection on Local WLC

This debug provides all the information related to the wired guest client.

debug client <mac-address>

```
Cisco Controller) > show debug
MAC address ..... 00:0d:60:5e:ca:62
Debug Flags Enabled:
 dhcp packet enabled.
 dot11 mobile enabled.
 dot11 state enabled
 dot1x events enabled.
 dot1x states enabled.
 pem events enabled.
 pem state enabled.
 (Cisco Controller) >Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  Adding mobile on Wired Guest 00:00:00:00:00(0)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  apfHandleWiredGuestMobileStation
  (apf_wired_guest.c:121) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:
00:00:00 from Idle to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Initializing policy
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Change state to AUTHCHECK (2) last state AUTHCHECK (2)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 AUTHCHECK (2)
  Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 L2AUTHCOMPLETE (4)
   Change state to DHCP_REQD (7) last state DHCP_REQD (7)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  apfPemAddUser2 (apf_policy.c:209) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:00:00 from Associated to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 Session Timeout is 0 -
  not starting session timer for the mobile
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Stopping deletion of Mobile Station: (callerId: 48)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
  Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Orphan Packet from 10.10.80.252
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
  Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
  Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
  DHCP_REQD (7) State Update from Mobility-Incomplete
   to Mobility-Complete, mobility role=Local
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) pemAdvanceState2 3934, Adding TMP rule
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
  DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00,
   slot 0, interface = 1, QOS = 0 ACL Id = 255,
   Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0 DHCP_REQD
   (7) Successfully plumbed mobile rule (ACL ID 255)
```

```
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
  Installing Orphan Pkt IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
  Unsuccessfully installed IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   0.0.0.0 Added NPU entry of type 9
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Sent an XID frame
Tue Sep 11 13:27:45 2007: 00:0d:60:5e:ca:62
  Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP xid: 0x87214d01 (2267106561), secs: 0, flags: 8000
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
        chaddr: 00:0d:60:5e:ca:62
  DHCP
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP
        ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP requested ip:10.10.80.252
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP ARPing for 10.10.110.1 (SPA 10.10.110.2, vlanId 110)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2
  VLAN: 110
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
  DHCP selected relay 2 - NONE
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
        op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
  DHCP
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
        xid: 0x87214d01 (2267106561), secs: 36957, flags: 8000
  DHCP
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2
```

```
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP requested ip: 10.10.80.252
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP sending REQUEST to 10.10.110.1 (len 350, port 1, vlan 110)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP selected relay 2 - NONE
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP setting server from OFFER
   (server 10.10.110.1, yiaddr 10.10.110.3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP transmitting DHCP OFFER (2)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP xid: 0x87214d01 (2267106561), secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
        ciaddr: 0.0.0.0, yiaddr: 10.10.110.3
  DHCP
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP
        siaddr: 0.0.0.0, giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP server id: 1.1.1.1 rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP received op BOOTREQUEST (1) (len 334, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP selecting relay 1 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
  gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP transmitting DHCP REQUEST (3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP
        op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP xid: 0x87214d01 (2267106561), secs: 36957, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP requested ip: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
        server id: 10.10.110.1 rcvd server id: 1.1.1.1
  DHCP
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP sending REQUEST to 10.10.110.1(len 374, port 1, vlan 110)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP selecting relay 2 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 -NONE
```

```
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  10.10.110.3 DHCP_REQD (7) Change state to WEBAUTH_REQD
   (8) last state WEBAUTH_REQD (8)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) pemAdvanceState2
   4598, Adding TMP rule
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  10.10.110.3 WEBAUTH_REQD (8) Replacing Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Successfully
  plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  Plumbing web-auth redirect rule due to user logout
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  Adding Web RuleID 31 for mobile 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  Assigning Address 10.10.110.3 to mobile
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP transmitting DHCP ACK (5)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
        op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
  DHCP
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP
        xid: 0x87214d01 (2267106561), secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP ciaddr: 0.0.0.0, yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
        siaddr: 0.0.0.0, giaddr: 0.0.0.0
  DHCP
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP server id: 1.1.1.1 rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  10.10.110.3 Added NPU entry of type 2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62 Sent an XID frame
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
  Username entry (guest1) created for mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
  Setting guest session timeout for mobile
   00:0d:60:5e:ca:62 to 79953 seconds
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Session Timeout is 79953 - starting session timer for the mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Change state to
   WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_NOL3SEC (14) Change state to RUN
   (20) last state RUN (20)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Reached PLUMBFA STPATH: from line 4518
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Replacing FastPath rule
type = Airespace AP Client
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
```

```
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3
   Added NPU entry of type 1
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 Sending a gratuitous
   ARP for 10.10.110.3, VLAN Id 110
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- <u>Configuring Auto-Anchor Mobility</u>
- Guest WLAN and Internal WLAN using WLCs Configuration Example
- External Web Authentication with Wireless LAN Controllers Configuration Example
- Cisco Wireless LAN Controller Configuration Guide, Release 4.2
- <u>Wireless Product Support</u>
- <u>Technical Support & Documentation Cisco Systems</u>