Konfigurationsbeispiel für kabelgebundenen Gastzugriff mit Cisco WLAN-Controllern

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Access Layer Switch-Konfiguration Wichtige Punkte für die Bereitstellung von kabelgebundenen Gastgeräten Plattformunterstützung Wireless LAN-Konfiguration Kabelgebundener Gastzugriff mit Anchor WLAN Controller Konfiguration des kabelgebundenen Gastclients Debugger für kabelgebundene Gastverbindungen auf lokalem WLC Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie den Gastzugriff mithilfe der neuen Funktion für kabelgebundenen Gastzugriff auf den Cisco WLAN Controllern (WLCs) konfigurieren, die Cisco Unified Wireless Software Version 4.2.61.0 und höher verwenden. Immer mehr Unternehmen erkennen die Notwendigkeit an, ihren Kunden, Partnern und Beratern beim Besuch ihrer Einrichtungen Internetzugang bereitzustellen. IT-Manager können Gästen über denselben Wireless LAN-Controller sicheren und kontrollierten Zugriff auf das Internet über kabelgebundene und Wireless-Netzwerke bereitstellen.

Gastbenutzer müssen die Möglichkeit haben, eine Verbindung zu bestimmten Ethernet-Ports herzustellen und auf das Gastnetzwerk zuzugreifen, wie vom Administrator konfiguriert, nachdem sie die konfigurierten Authentifizierungsmethoden abgeschlossen haben. Wireless-Gastbenutzer können über die aktuellen Gastzugriffsfunktionen problemlos eine Verbindung zu den WLAN-Controllern herstellen. Darüber hinaus bietet das Wireless Control System (WCS) zusammen mit der grundlegenden Konfiguration und Verwaltung der WLAN-Controller erweiterte Gastbenutzerdienste. Kunden, die bereits WLAN-Controller und WCS in ihrem Netzwerk implementiert haben oder planen, können dieselbe Infrastruktur für den kabelgebundenen Gastzugriff nutzen. So wird Endbenutzern ein einheitlicher, kabelgebundener und Wireless-Gastzugriff ermöglicht.

Kabelgebundene Gastports werden an einem festgelegten Standort bereitgestellt und an einen Access Switch angeschlossen. Bei der Konfiguration auf dem Access Switch befinden sich diese Ports in einem der kabelgebundenen Layer-2-VLANs für Gäste. Den Kunden stehen zwei separate Lösungen zur Verfügung:

- Ein einzelner WLAN-Controller (VLAN Translation Mode) Der Access Switch leitet den kabelgebundenen Gastdatenverkehr im Gast-VLAN an den WLAN-Controller weiter, der die kabelgebundene Gastzugangslösung bereitstellt. Dieser Controller übernimmt die VLAN-Übersetzung vom Eingangs-VLAN für kabelgebundene Gäste zum Ausgangs-VLAN.
- Zwei WLAN-Controller (Auto-Anchor-Modus): Der Access Switch leitet den kabelgebundenen Gastdatenverkehr an einen lokalen WLAN-Controller (den Controller, der dem Access Switch am nächsten liegt) weiter. Dieser lokale WLAN-Controller verankert den Client an einem DMZ-Anker-WLAN-Controller (Demilitarized Zone), der für den kabelgebundenen und Wireless-Gastzugriff konfiguriert ist. Nach erfolgreicher Übergabe des Clients an den DMZ-Anker-Controller werden die DHCP-IP-Adresszuweisung, die Client-Authentifizierung usw. im DMZ-WLC behandelt. Nach Abschluss der Authentifizierung kann der Client Datenverkehr senden/empfangen.



Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Unterstützung der Funktion für kabelgebundenen Gastzugriff auf den Cisco WLAN-Controllern wird von der Cisco Unified Wireless Software Version 4.2.61.0 und höher unterstützt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Access Layer Switch-Konfiguration

Um den kabelgebundenen Gastzugriff bereitzustellen, müssen die Ports im Access Layer-Switch für Layer 2 vom Administrator im Gast-VLAN konfiguriert werden. Das Gast-VLAN muss von allen anderen VLANs getrennt sein, die auf diesem Switch konfiguriert sind. Der Gast-VLAN-Datenverkehr wird an den nächsten lokalen WLAN-Controller weitergeleitet. Der lokale Controller leitet den Gastdatenverkehr über einen Ethernet over IP (EoIP)-Tunnel an einen DMZ Anchor-Controller weiter. Diese Lösung erfordert mindestens zwei Controller.

Alternativ dazu übersetzt der Access Switch das Gast-VLAN mit dem einzelnen Controller in die Ausgangsschnittstelle des WLAN-Controllers.

cat6506# show vlan id 49 VLAN Name Status Ports _____ _____ 49 VLAN0049 active Gi2/1, Gi2/2, Gi2/4, Gi2/35 Gi2/39, Fa4/24 VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 ____ _____ 1500 - -49 enet 100049 _ _ 0 0 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

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Wichtige Punkte für die Bereitstellung von kabelgebundenen Gastgeräten

- Derzeit werden fünf Gast-LANs für den kabelgebundenen Gastzugriff unterstützt. Insgesamt können im Anchor-WLC 16 WLANs für Wireless-Benutzer und 5 WLANs für kabelgebundenen Gastzugriff konfiguriert werden. Für WLANs gibt es keine separaten Tunnel. Alle Gast-WLANs, einschließlich der WLANs für kabelgebundenen Gastzugriff, verwenden dieselben EoIP-Tunnel zum Anchor-WLC.
- Administratoren müssen dynamische Schnittstellen im WLAN-Controller erstellen, sie als "Gast-LAN" markieren und sie mit WLANs verknüpfen, die als Gast-LANs erstellt wurden.
- Stellen Sie sicher, dass die WLAN-Konfigurationen einschließlich der Authentifizierung auf dem Anker- und Remote-Controller identisch sind, um den Client-Datenverkehr weiterzuleiten.
- WLCs sollten über kompatible Softwareversionen verfügen. Stellen Sie sicher, dass die gleiche Hauptversion ausgeführt wird.
- Die Webauthentifizierung ist der Standardsicherheitsmechanismus, der in einem kabelgebundenen Gast-LAN verfügbar ist. Folgende Optionen sind derzeit verfügbar: Offen, Webauthentifizierung und Webpassthrough.
- Falls der EoIP-Tunnel zwischen dem Remote- und Anker-WLC ausfällt, wird die Client-Datenbank vom Anchor-WLC entfernt. Der Kunde muss sich erneut zuordnen und authentifizieren.
- Es wird keine Layer-2-Sicherheit unterstützt.
- Multicast-/Broadcast-Datenverkehr in den LANs für kabelgebundene Gäste wird verworfen.
- Die DHCP-Proxy-Einstellungen müssen auf dem Anker- und dem Remote-Controller identisch sein.

Für den kabelgebundenen Gast wird im Controller ein Timeout für Inaktivität ausgeführt. Wenn innerhalb der konfigurierten Zeit keine Pakete vom Client empfangen werden, wird der Client vom Controller entfernt. Wenn ein Client beim nächsten Mal eine ARP-Anforderung (Address Resolution Protocol) sendet, wird ein neuer Clienteintrag erstellt und entsprechend der Sicherheitskonfiguration in den Web Auth/Run-Status verschoben.

Plattformunterstützung

Der kabelgebundene Gastzugriff wird auf folgenden Plattformen unterstützt:

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

Wireless LAN-Konfiguration

In diesem Beispiel wird von der grundlegenden Konfiguration des Wireless LAN-Controllers ausgegangen. Der Schwerpunkt liegt auf der zusätzlichen Konfiguration, die für die Implementierung des kabelgebundenen Gastzugriffs erforderlich ist.

 Erstellen Sie eine dynamische Schnittstelle, und markieren Sie sie als "Gast-LAN". Wenn Sie diese dynamische Schnittstelle in der aktuellen Version erstellen, müssen Sie eine IP-Adresse und ein Standard-Gateway angeben, auch wenn diese Schnittstelle nicht vorhanden ist, da es sich um ein Layer-2-VLAN handelt. Sie müssen keine DHCP-Adresse angeben.

Kabelgebundene Gastclients sind physisch mit diesem VLAN verbunden.

	araaraaan							949999
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Interface	s > Edit						
General Inventory	General I	nformati	on					
Interfaces	Interface	Name	wired-vl	an-49				
Multicast Network Routes	MAC Add	ress	00:18:b	9:ea:a7:23				
Internal DHCP Server	Interface	Address						
Mobility Management	VLAN Ide	ntifier	49					
Ports	IP Addres	ss	10.10).49.2				
NTP	Netmask		255.2	255.255.0				
▶ CDP	Gateway		10.10	0.49.1				
Advanced	Physical I	informati	on					
	Port Num	ber	1]				
	Backup P	ort	0]				
	Active Po	rt	1					
	Enable D Managem	ynamic AP tent						
	Configura	tion						
	Quarantir	ne				-		
	Guest Lar	n	V					
	DHCP Info	ormation						
	Primary I	DHCP Serve	er 🗌					
	Secondar	γ DHCP Se	rver					
	Access Co	ontrol Lis	t					
	ACL Nam	e	none					
	Note: Chang temporarily some clients	ing the Inti disabled ar 1.	erface parameters of thus may result	causes the WL in loss of conn	ANs to be ectivity for			

2. Erstellen Sie eine weitere dynamische Schnittstelle, über die die kabelgebundenen Gastclients eine IP-Adresse erhalten. **Hinweis**: Sie müssen in dieser Schnittstelle eine IP-Adresse, ein Standard-Gateway und eine DHCP-Serveradresse angeben.

ahah								
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Interface	s > Edit						
General Inventory	General I	nformatio	on					
Interfaces	Interface	Name	110					
Multicast	MAC Add	ress	00:18:b	9:ea:a7:23				
Network Routes								
Internal DHCP Server	Interface	Address						
Mobility Management	VLAN Ide	ntifier	110					
Ports	IP Addre:	ss	10.10	.110.2				
NTP	Netmask		255.2	55.255.0				
▶ CDP	Gateway		10.10	.110.1				
Advanced	Physical I	nformati	on					
	Port Num	ber	1					
	Backup P	ort	0					
	Active Po	rt	1					
	Enable D Managem	ynamic AP ient						
	Configura	tion						
	Quarantir	ne						
	Guest Lar	n						
	DHCP Info	ormation						
	Primary (DHCP Serve	10.10	.110.1				
	Secondar	y DHCP Se	rver					
	Access Co	ontrol Lis	t					
	ACL Nam	e	none		*			
	Note: Chang temporarily some clients	ing the Inti disabled ar	arface parameters id thus may result	causes the WL in loss of conn	ANs to be ectivity for	-		

3. Dies sind die dynamischen

Schnittstellen:

cisco		<u>w</u> lans		WIRELESS	<u>S</u> ECURITY	MANAGEMENT CO	MMANDS HELP	
Controller	Interfaces							
General	Interface N	Name		/LAN Identifier	IP Address	Interface Type	Dynamic AP Management	
Inventory	110		1	110	10.10.110.2	Dynamic	Disabled	-
Interfaces	ap-manager		U	untagged	10.10.80.4	Static	Enabled	
Multicast	managemen	5	L	untagged	10.10.80.3	Static	Not Supported	
Network Routes	service-port			1/A	0.0.0.0	Static	Not Supported	
Internal DHCP Server	virtual		P	ŧ∕A	1.1.1.1	Static	Not Supported	
Mobility Management	wired-vlan-4	19	4	19	10.10.49.2	Dynamic	Disabled	-
Ports								

4. Hinzufügen eines neuen WLANs: Type=Gast-

LAN

Cisco_48:53:c3 - Microso	R Internet Explorer			1993 - Carlos				10 ×
File Edk Veve Favorites	Toole Help			2.2.2.2.2.2				200
3m · () · 1	2 🏠 🔎 Search 😭	Favortes 🧑 💡	3· 3- 173	24				Links ."
Address Address Address Address	204/screens/frameivet.html	************			**********			• 🖸 •
սիսիս						Saye Co	nfiguration (Emg.	Logout : Enfresh
cisco	MONITOR MUNIS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	영화장양장등을 관
WLANs	WLANs > New						< Back	Apply
* WLANS	Туре	Guest LAN						
Advanced	Profile Name	Wired-Gues	t					
	WLAN SSID	Wined-Gues	1					

5. Aktivieren Sie das WLAN. Ordnen Sie die Eingangs-Schnittstelle dem in Schritt 1 erstellten "Gast-LAN" zu, und die Ausgangsschnittstelle kann eine Verwaltungsschnittstelle oder eine andere dynamische Schnittstelle sein, vorzugsweise aber eine dynamische Schnittstelle, wie sie in Schritt 2 erstellt

wurde.	dt Internet Explorer				3 [5]
File Edit View Feverte	e Teols Help				1
🕒 Sack + 🐑 / 💌	🗟 🐔 🔎 Search 🔮 Fave	rtes 🙆 🍰 😓 🗔 🗍	11		Links
Address () https://10.77.24	1.204/screens/frameset.html				- 🔁 😡
cisco	MONITOR MLANIS C	ONTROLLER WIRELESS SEC	URITY MANAGEMENT C	Sage Configuration Elina . QMMANDS HELP	Logout Enfresi
WLANs	WLANs > Edit		<u> </u>	< Back	Apply
* WLANS WLATES	General Security	QoS Advanced			
Advanced	Profile Name Type	Wired-Gunst Gunst LAN			
	SSID	Wired-Güein			
		r Enabled			
	Security Policies	Web-Auth (Modifications done under secur	ity tab will appear after applyi	ng the changes.)	
	Ingress Interface	wired-vian-49 -			
	Egress Interface	management 💌			
	anti pondentri productiona				
	Foot Notes	GUNTANA ANG ANG ANANA ANG ANG ANG ANG ANG AN	ARTER ART 200 TEN ANN AND ART 3	<u>ne de la dela de la dela dela dela dela d</u>	
	2 Web Policy cannot be 4 When olient exclusion	used in combination with IPsec is enabled, a Timeout Value of zero	means infinity (will require ad	ministrative override to reset ex	oluded clients)
and the second of the	. 265				

6. Die Webauthentifizierung ist standardmäßig als Sicherheitsoption im Gast-LAN aktiviert. Sie kann in *None* oder *Web Passthrough* geändert werden.



7. Dies ist die endgültige Konfiguration des

WLANs.						
Cisco_48:53c3 - Microsoft)	Internet Diplorer					_@×
File Edit View Favorites	Tools Help					
🔇 Bick, + 😥 - 💌 💈) 🏠 🔎 Search 🔥 7	'avortas 🧭 🍰 🕄 🕻	TR 🖵 🛍			Linka ³⁹
Address () https://10.77.244.20	H/screens/frameset.html					💌 🛃 🖘
- abala -				Saye	Configuration Ping Lo	gout Eefresh
CISCO	MONITOR WLANS	CONTROLLER WIRELES	S SECURITY MANAGEMEN	T COMMAND	s HELP	
WLANs	WLANs.				N	ew
WEANS				Admin		
WLANS	Profile Name	Type Wi	LAN SSID	Status	Security Policies	
Advanced	Simeb.	WLAN ter	web	Enabled	[WPA2][Auth(802.1×)]	
	Wined-Guest	Guest LAN Wi	red-Guest	Enabled	Web-Auth	-

8. Fügen Sie in der lokalen Datenbank des WLC einen Gastbenutzer hinzu.

ware fail unbelieters verso	dan en el u eneser nom					4 4 4 4	
cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MONAGEMENT	Sage Co COMMANDS	HELP	Logout Refr
ARA General Caneral RAD1US Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Local Net Users > 8 User Name Password Confirm Password Lifetime (seconds) Guest User Role Creation Time Remaining Time WLAN Profile	Edit guest ••••• 86400 Thu Nov 20 14:12:3 23 h 59 m 56 s Wined-Guest (c)	2 2908)		< 8atk	Apply
Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced	Description	(Wired-guest		L			

Im Ausland müssen Sie den Eingang als konfiguriertes "Gast-LAN" festlegen. Am Ausgang müssen Sie eine Schnittstelle festlegen, möglicherweise die Management-Schnittstelle. Sobald der EoIP-Tunnel erstellt wurde, wird der Datenverkehr jedoch automatisch über den Tunnel anstatt über die Management-Adresse gesendet.

Kabelgebundener Gastzugriff mit Anchor WLAN Controller

In diesem Beispiel lautet die IP-Adresse des Remote-Wireless LAN-Controllers 10.10.80.3 und die IP-Adresse des Anchor DMZ-Controllers 10.10.75.2. Beide sind Teil zweier unterschiedlicher Mobilitätsgruppen.

1. Konfigurieren Sie die Mobilitätsgruppe des Anker DMZ-Controllers, wenn Sie die MAC-Adresse, die IP-Adresse und den Namen der Mobilitätsgruppe des Remote-Controllers hinzufügen.

and the base of the second								
CISCO		<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 Anchor Config	Mobility O This page al Mobility ground mobility ground address and spaces.	WLANS Group Me lows you to up member up member l group nam l group nam de: 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	WIRELESS group members , one per line. B s a MAC addres ated by one or n bile-10	secontry Each as, IP more		COMMANDS	HED
Ports					-			
Ports					*			
▶ CDP								
Advanced								

2. Konfigurieren Sie auf ähnliche Weise die Mobilitätsgruppe im Remote-

Controller.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Mobility G	Group Me	embers > Edi	t All				
General Inventory Interfaces Multicaet	This page al Mobility grou mobility grou address and spaces.	Jows you to up member up member I group nam	e edit all mobility s are listed belov is represented a ne(optional) sepa	group members v, one per line. I s a MAC addres rated by one or	at once. Each ss, IP more			
Network Routes	00:18:b9:e 00:18:73:3	a:a7:20 4:b2:60	10.10.80.3 10.10.75.2 m	obile-9	<u> </u>			
 Mobility Management Mobility Groups Mobility Anchor Config 								
Ports NTP					T			
CDP Advanced								

3. Erstellen Sie das kabelgebundene WLAN mit dem genauen Namen im Anchor-WLC. Die Eingangs-Schnittstelle ist in diesem Fall "none", da logischerweise die Eingangs-Schnittstelle der EoIP-Tunnel vom Remote-Controller ist. Die Ausgangsschnittstelle ist eine andere Schnittstelle, über die die kabelgebundenen Clients die IP-Adresse empfangen. In diesem Beispiel wird eine dynamische Schnittstelle mit dem Namen *guest* erstellt. In diesem Stadium können Sie das WLAN jedoch nicht aktivieren, da eine Fehlermeldung angezeigt wird, die besagt, dass eine Eingangsschnittstelle nicht *unbeschränkt* sein kann.



4. Konfigurieren Sie die Layer-3-Sicherheit als *Webauthentifizierung*, ähnlich dem Remote-Controller.

and the second		Transie (Marine St.
CISCO	HONITOR HUNNIN CONTROLLER WIRELESS SECURITY MYNASAMENT COMMUNIS HELP	
WLANs WLANs WLANS F Advanced	WLAND > Edit Control Security Qets Advanced Career 3 Advanced Larer 3 Advanced Larer 3 Advanced Larer 3 Advanced Control Production on Advanced Control	Apply

5. Erstellen Sie den Mobilitätsanker am Anker-Controller, und ordnen Sie ihn sich selbst

20.								
cisco	NONILOW BEAM	NTROLLER MIR	euess geouante i	NORMENT COMMAN	6 HELF		54)	a Configuration (Sing Lingsof Batterit
WLANS	WLANs							New
* WLANS	Profile Name	Туре	WLAN SSID	Admin Status	Security Policies			
k Advanced	94	Windless	ф.	Enabled	Web-Auth			
	<u>a</u> 2	Wireless	92	Enobled	Web-Auth			
	al and a state	Wined	and count	Enabled	Web-Auth			
	Michaelle.	*****	weets-garre.	Contraction	1010-00101	Fachove		
all all all		CONTRACTOR OF THE OWNER.						e Colfiguration II Des I suggest l'Artest
CISCO	BORITOR WARE CO	NTROLLER W/F	ELESS SECURITY I	NUMBERENT COMMAND	с нејз			
WLANs	Nobility Anchore							< Mack
- WLANE	WLAN SSID Hired-	quert						
b Advanced	Switch IP Address (Andree)					Data Path	Control Path	
	local				18			•
	Nakiday Arachar Cr	vale						
	Switch IP Address (Ar	ichor)	10.39.40.3 8					

 Wenn der Mobilitätsanker erstellt wurde, kehren Sie zur
ück, und aktivieren Sie das kabelgebundene WLAN.



7. Erstellen Sie auf ähnliche Weise den Mobilitätsanker auf dem Remote-WLC für das kabelgebundene Gast-

ANs	WLANs						Here
WLANS	Profile Name	Type	WLAN SSID	Admin Status	Security Policies		
WLARE	ai.	Windows	φň.	Enabled	Web-Auth		
Advanced	<u>a</u> 2	Windless	b 5	Enabled	Web-Auth		
	4	Wireless	q3	Disabled	Web-Auth		
	winds.control.	Wined	wired-guest.	Exobled	Web-Auth	Fathere	
						Margary .	
						ALC: N	

Wählen Sie die IP-Adresse des Anker-WLC aus, und erstellen Sie den Mobilitätsanker.

Sector In Instant				
CISCO	BONITOR WORKS CONTROLLER WIRELESS SECURITY PRINCEMENT COM	eeroo Haya		
WLANs	Nobility Anchora			< mack
* WLANS	WLAN SSID wired-guest			
+ Advanced	Switch IF Address (Anchor)	Data Path	Control Path	
> Advanced	Nextsh IP Address (Anchor) 20.18.78.2	Data Path 10	Control Path up	
+ Advanced	twitch IP Address (Anchor) 20.18 /%.2 76.64819, Anchor Create	Data Path sp	Control Path 19	•

Überprüfen Sie, ob der Daten- und Steuerungspfad aktiv ist. Falls nicht, stellen Sie sicher, dass diese Ports zwischen dem Anker und dem Remote-Wireless LAN-Controller offen sind: UDP 1666 oder IP 97.

 Wenn ein kabelgebundener Gastbenutzer mit dem Switch verbunden ist und die Webauthentifizierung abgeschlossen hat, muss der Status "Policy Manager" ausgeführt werden, und die Rolle "Mobility" lautet "Export Foreign" (Ausländisch exportieren).

				Saye Configuration Fing Logout Refree
CISCO	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY	MANAGEMENT COMM	MANDS 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	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
	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

Überprüfen Sie auf ähnliche Weise den Status im Anchor-WLC. Der Status "Policy Manager" muss "RUN" lauten, und die Mobilitätsrolle "Export

Anchor".				
cisco	MONITOR WLANS CON	roller wireless secu	RITY MANAGEMENT COMM	iave Configuration Eing Logout Befre MNDS HELP
Monitor Summary	Clients > Detail		< Back	Apply Link Test Remove
Access Points Statistics CDP Rogues	MAC Address IP Address Client Type	00:0d:60:5e:ca:62 10.10.77.11 Regular	AP Address AP Name AP Type WIAN Profile	Unknown 10.10.80.3 Mobile wired-quest-1
Clients Multicast	Port Number Interface VLAN ID	1 guest 77	Status Association ID 802.11 Authentication	Associated 0 Open System
	CCX Version E2E Version Mobility Role	Nat Supported Nat Supported Export Anchor	Reason Code Status Code CF Pollable	0 0 Not Implemented
	Mobility Peer IP Address Policy Manager State Mirror Mode	10.10.80.3 RUN Disable 💌	CF Poll Request Short Preamble PBCC	Not Implemented Not Implemented Not Implemented
	Protection	No	Channel Agility Timeout	Not Implemented

Konfiguration des kabelgebundenen Gastclients

Der kabelgebundene Gast-Client erhält eine IP-Adresse vom Ausgangs-VLAN, kann jedoch keinen Datenverkehr weiterleiten, bis der Webauthentifizierungsprozess abgeschlossen ist.

Um sich als Gastbenutzer anzumelden, gehen Sie wie folgt vor:

 Öffnen Sie ein Browserfenster, und geben Sie den gewünschten URL-Namen ein (z. B. www.cisco.com). Wenn die Webauthentifizierung aktiviert ist, wird der Gast auf die Standardwebseite des Wireless LAN-Controllers umgeleitet, und für die eingegebene URL kann eine DNS-Auflösung vorgenommen werden. Geben Sie andernfalls die folgende URL ein: https://1.1.1.1/login.html, wobei die IP-Adresse 1.1.1.1 die virtuelle IP-Adresse des Wireless LAN-Controllers

ist.			
Web Authentication - A	kicrosoft Internet Explorer		C 6 🛛
File Edit View Favorites	Tools Help		A 8
Ġ tack + 🕤 + 🖹	🗟 🏠 🔎 Search 👷 Favorites 🤣 🎯 - 🌺 💬 🍪 💷		
Address 🛃 https://1.1.1.1/log	jn.html	🔁 🙃	Linis 🎽 🥌 Snegit 🛐 🛃
Google G-	😼 Go o 🤣 🛃 👻 🏠 Bookmarks 🕶 🥸 O blocked 🛛 🍄 Check 💌 🐴 AutoLink 👻 🔚 AutoFill 🍙 Send to 🕶	6	🕥 Settings 🕶
Login			
Welcome to the C	Sisco wireless network		
Cisco is pleased to pr for your network. Pleas	ovide the Wireless LAN infrastructure se login and put your air space to work.		
User Name	guesti		
Password			
1	Submit		
街 Done			🚔 🔵 Internet

- 2. Geben Sie den angegebenen Benutzernamen und das angegebene Kennwort ein.
- 3. Wenn die Anmeldung erfolgreich war, wird dies in einem Browserfenster
 - angezeigt.



Debugger für kabelgebundene Gastverbindungen auf lokalem WLC

Dieses Debuggen stellt alle Informationen zum kabelgebundenen Gastclient bereit.

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

debug client

```
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
   DHCP chaddr: 00:0d:60:5e:ca:62
```

```
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
  DHCP
        op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
  DHCP xid: 0x87214d01 (2267106561), secs: 36957, flags: 8000
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
        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
  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
        requested ip: 10.10.110.3
  DHCP
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
  DHCP
        server id: 10.10.110.1 rcvd server id: 1.1.1.1
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
```

```
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
  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 quest 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, 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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Konfigurieren von automatischer Ankermobilität
- Gast-WLAN und internes WLAN mit WLCs Konfigurationsbeispiel
- Konfigurationsbeispiel für die externe Webauthentifizierung mit Wireless LAN-Controllern

- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.2
- <u>Wireless-Produktunterstützung</u>
- Technischer Support und Dokumentation Cisco Systems