Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Configuration du commutateur d'accès au réseau Points importants pour un déploiement par câble pour invité Prise en charge de la plate-forme Configuration du réseau local sans fil (WLAN) Accès par câble pour invité avec contrôleur d'ancrage WLAN Configuration par câble du client invité Dépannage de la connexion par câble pour invité sur un contrôleur WLAN local Vérification Dépannage

Introduction

Le présent document décrit comment configurer l'accès invité au moyen de la nouvelle fonctionnalité d'accès par câble pour invité sur les contrôleurs WLAN de Cisco qui utilisent la version 4.2.61.0 du logiciel sans fil unifié de Cisco ou une version ultérieure. Un nombre croissant d'entreprises reconnaissent l'importance de fournir un accès Internet à leurs clients, à leurs partenaires et à leurs consultants lorsqu'ils visitent leurs installations. Les gestionnaires des TI peuvent fournir un accès par câble ou sans fil, sécurisé et contrôlé, permettant aux invités d'accéder à Internet sur le même contrôleur de réseau local sans fil.

Les utilisateurs invités pourront se connecter aux ports Ethernet désignés et accéder au réseau invité configuré par l'administrateur après avoir franchi les mesures d'authentification configurées. Les utilisateurs invités sans fil peuvent facilement se connecter aux contrôleurs WLAN par l'intermédiaire des fonctions actuelles d'accès invité. De plus, le système de contrôle sans fil (WCS) ainsi que la configuration de base et la gestion des contrôleurs WLAN offrent une expérience améliorée aux utilisateurs invités. Les clients qui ont déjà déployé ou qui prévoient déployer des contrôleurs WLAN et le système WCS dans leur réseau peuvent utiliser la même infrastructure pour l'accès par câble pour invité. Ainsi, les utilisateurs finaux pourront profiter d'une expérience d'accès invité uniforme, qu'ils utilisent une connexion sans fil ou par câble.

Les ports câblés pour invité sont accessibles à un endroit désigné et sont branchés sur un commutateur d'accès. Selon la configuration du commutateur d'accès, ces ports sont associés à l'un des réseaux locaux virtuels (VLAN) de la couche 2 de l'accès invité par câble. Deux solutions s'offrent aux clients :

- Un seul contrôleur WLAN (mode « VLAN Translation ») le commutateur d'accès relie le trafic de l'invité par câble sur le réseau VLAN d'invité au contrôleur WLAN qui assure la solution d'accès par câble pour invité. Ce contrôleur effectue la traduction VLAN du réseau VLAN d'entrée par câble pour invité vers le réseau VLAN de sortie.
- Deux contrôleurs WLAN (mode « Auto Anchor ») le commutateur d'accès relie le trafic de l'invité par câble à un contrôleur WLAN local (le contrôleur le plus près du commutateur d'accès). Ce contrôleur WLAN local connecte le client à un contrôleur WLAN d'ancrage dans une zone démilitarisée (DMZ) qui est configuré pour prendre en charge un accès invité par câble et sans fil. Après avoir dirigé le client vers la zone démilitarisée du contrôleur d'ancrage, le système traite l'attribution de l'adresse IP au serveur DHCP, l'authentification du client et ainsi de suite. Lorsque le processus d'authentification est terminé, le client peut envoyer et recevoir du trafic.



Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

La fonctionnalité d'accès par câble pour invité sur les contrôleurs WLAN de Cisco est offerte dans la version 4.2.61.0 du logiciel sans fil unifié de Cisco et dans les versions ultérieures.

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.

Configuration

cat6506# show vlan id 49

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Configuration du commutateur d'accès au réseau

Afin d'assurer un accès par câble à l'invité, l'administrateur doit configurer les ports désignés du commutateur d'accès au réseau de la couche 2 sur le réseau VLAN pour invité. Le réseau VLAN pour invité doit être séparé de tous les autres réseaux VLAN configurés sur ce commutateur. Le trafic du réseau VLAN pour invité est acheminé au contrôleur WLAN local le plus près. Le contrôleur local achemine le trafic de l'invité par l'entremise d'un tunnel Ethernet sur IP (EoIP) vers un contrôleur d'ancrage de zone démilitarisée. Il faut au moins deux contrôleurs pour cette solution.

Par ailleurs, le commutateur d'accès relie le réseau VLAN pour invité au contrôleur, qui traduit ce réseau vers l'interface de sortie du contrôleur WLAN.

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 - -0 49 enet 100049 _ _ -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

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Points importants pour un déploiement par câble pour invité

- Actuellement, cinq réseaux locaux pour invités sont pris en charge pour l'accès invité. Au total, 16 réseaux WLAN pour les utilisateurs sans fil et 5 réseaux WLAN pour les invités par câble peuvent être configurés sur le contrôleur WLAN d'ancrage. Il n'y a pas de tunnel distinct pour les réseaux WLAN. Tous les réseaux WLAN invités, y compris les réseaux WLAN à accès pour invité par câble, utilisent les mêmes tunnels EoIP connectés au contrôleur WLAN d'ancrage.
- Les administrateurs doivent créer des interfaces dynamiques dans le contrôleur WLAN, les marquer comme " LAN invité, les " et les associer aux WLAN créés en tant que LAN invité.
- Assurez-vous que les configurations WLAN, y compris le processus d'authentification, sont identiques sur les contrôleurs d'ancrage et sur les contrôleurs à distance afin d'assurer le transfert du trafic client.
- Les contrôleurs WLAN doivent avoir des versions logicielles compatibles. Assurez-vous qu'ils utilisent la même version principale.
- L'authentification Web est le mécanisme de sécurité par défaut disponible sur un réseau local invité par câble. Les options disponibles sont les suivantes : « Open » (ouvert), « Web Auth » (authentification Web) et « Web Passthrough » (intercommunication Web).
- En cas d'échec de connexion par tunnel EoIP entre le contrôleur WLAN d'ancrage et le contrôleur à distance, la base de données du client est effacée du contrôleur WLAN d'ancrage. Le client doit alors relancer les étapes d'association et d'authentification.
- Aucune sécurité pour la couche 2 n'est prise en charge.
- Le trafic de diffusion/multidiffusion du réseau local invité par câble est supprimé.
- Les paramètres du serveur mandataire DHCP doivent être identiques sur les contrôleurs d'ancrage et sur les contrôleurs à distance.

Avec un accès invité par câble, aucun délai d'inactivité n'est en fonction dans le contrôleur. Si aucun paquet n'est reçu pendant la période configurée par le client, ce dernier est retiré du contrôleur. Au prochain envoi d'une demande de protocole de résolution d'adresse (ARP) par le client, une nouvelle entrée de client est créée et l'état passe à « Web Auth/RUN », conformément à la configuration de sécurité.

Prise en charge de la plate-forme

L'accès par câble pour invité est pris en charge sur ces plateformes :

 Contrôleur WLAN 4402, 4404, WiSM, 3750G, 5508, WiSM2, contrôleur WLAN virtuel de Cisco

Configuration du réseau local sans fil (WLAN)

Dans l'exemple suivant, on emploie par défaut la configuration de base du contrôleur de réseau local sans fil. On se concentre sur la configuration supplémentaire requise pour mettre en œuvre l'accès par câble pour invité.

1. Créez une interface dynamique et marquez-la comme un réseau local invité ". " Dans la

version actuelle, lorsque vous créez une interface dynamique, vous devez fournir une adresse IP et une passerelle par défaut même s'il n'y en a pas, puisqu'il s'agit d'un réseau VLAN de la couche 2. Vous ne devez pas fournir n'importe quelle adresse DHCP. Les clients invités sont physiquement connectés par câble à ce réseau VLAN.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Interfaces	s > Edit						
General Inventory	General I	nformatio	n					
Interfaces	Interface	Name	wired-vl	an-49				
Multicast	MAC Add	ress	00:18:b	9:ea:a7:23				
Network Routes	Interface	Addross						
Internal DHCP Server	Interface	Auuress		-				
P Moonity Management	VLAN Ide	ntifier	49					
NTD	IP Addres	55	10.10	0.49.2				
► CDP	Netmask		255.2	55.255.0				
Advanced	Gateway		10.10	.49.1				
	Physical I	nformati	on					
	Port Num	ber	1					
	Backup P	ort	0					
	Active Po	rt	1					
	Enable Dy Managem	ynamic AP ient						
	Configura	tion						
	Quarantin	1e						
	Guest Lar	ı	V					
	DHCP Info	ormation						
	Primary D	DHCP Serve	er 📃					
	Secondar	y DHCP Se	rver					
	Access Co	ontrol Lis	t					
	ACL Nam	e	none					
	Note: Chang temporarily some clients	ing the Inte disabled an	erface parameters d thus may result	causes the WL in loss of conn	ANs to be ectivity for			

2. Créez une autre interface dynamique où les clients invités par câble reçoivent une adresse IP.**Note**: Vous devez fournir une adresse IP, une passerelle par défaut ou une adresse de serveur DHCP pour cette interface.

ahaha								
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Interfaces	s > Edit						
General Inventory	General I	nformatio	on					
Interfaces	Interface	Name	110					
Multicast Network Routes	MAC Add	ress	00:18:b	9:ea:a7:23				
Internal DHCP Server	Interface	Address						
Mobility Management	VLAN Ide	ntifier	110]				
Ports	IP Addres	s	10.10	.110.2				
NTP	Netmask		255.2	55.255.0				
P CDP	Gateway		10.10	.110.1				
P Advanced	Physical I	nformati						
	Port Num	ber	1					
	Backup P	ort	0					
	Active Po	rt	1					
	Enable Dy Managem	ynamic AP ient						
	Configura	tion						
	Quarantin	e						
	Guest Lar	n						
	DHCP Info	ormation						
	Primary D	DHCP Serve	er 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 Inte disabled ar	arface parameters id thus may result	causes the WL in loss of conn	ANs to be ectivity for			

3. Voici les interfaces

dynamiques :

cisco	MONETOR WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT CON	MMANDS HELP	
Controller	Interfaces						
General	Interface Name	v	LAN Identifier	IP Address	Interface Type	Dynamic AP Management	
Inventory	110	11	10	10.10.110.2	Dynamic	Disabled	-
Interfaces	ap-manager	ur	ntagged	10.10.80.4	Static	Enabled	
Multicast	management	ur	ntagged	10.10.80.3	Static	Not Supported	
Network Routes	service-port	N	/A	0.0.0.0	Static	Not Supported	
Internal DHCP Server	virtual	N/	/A	1.1.1.1	Static	Not Supported	
Mobility Management	wired-vlan-49	45	9	10.10.49.2	Dynamic	Disabled	-
Ports							

4. Ajoutez un nouveau réseau WLAN : Type = Guest LAN (réseau local pour invités).

Cisco_48:53:c3 - Microso	A Internet Explorer			and the second s				ale X
File Edit. View Pavyrites	i Toole Help							an 1997 a 19
3m · () · 1	🔊 🏠 🔎 Search 😭	lavortes 🧑 💡	3· 🏷 🗔	24				Links "
Address Ntps://10.77.244	204/screens/frameset.html	************			*********			• 🔁 🕤
ahaha						Saye Co	nfiguration (Emg.	Logout : Befresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	22222222
WLANs	WLANs > New						< Back	Apply
* WLANS	Туре	Guest LAN						
Advanced	Profile Name	Wired-Gues	t					
	WLAN SSID	Wined-Gues	٩					

5. Activez le réseau WLAN : mappez l'interface d'entrée à l'" de réseau local invité " créée à l'étape 1, et l'interface de sortie peut être une interface de gestion ou toute autre interface dynamique, bien que de préférence une interface dynamique telle que celle créée à l'étape 2.

	Seaton X Favor	• • • • • • • • • • • • • • • • • • •	UPIS
tehens 👔 https://10.77.244	.204/screens/Frameset.html		I 🖬 🖬
cisco	MONITOR WLANE CO	SALA CONTIGUAR NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	ion Elog Lagout Batra I
MLANs	WLANs > Edit	110	C Back Apply
WLANS WLANS WLANS Advanced	General Security Profile Name Type SSED Status Security Policies Egress Interface Egress Interface	QoS Advanced Wired-Guent Guent LAN Wored-Guent P Enabled P Web-Auth P (Modifications done under security tob will appear after applying the changes.) wired-rian-49 * management *	
	Foot Notes 2 Web Policy cannot be u 4 When client exclusion in	sed in combination with IPsec : enabled, a Timeout Value of zero means infinity (will require administrative overrid	le to reset evoluded clients)

6. L'option « Web authentication » (authentification Web) est activée par défaut comme option de sécurité configurée sur le réseau local pour invités. Cette option peut être modifiée à « None » (aucun) ou « Web Passthrough » (intercommunication Web).



7. Voici la configuration finale du

réseau WLAN.									
Cisco_48:53:c3 - Microsoft Inte	met Diplorer								X
File Edit View Favorites Too	is Help								
🔇 Back, 🔹 😥 - 💽 😰 🤇	🏠 🔎 Sea	nh 📩 P	avortas 🧭	i 🍰 👌	a 🖙 🔜 🏭				Links ³⁹
Address () https://t0.77.244.204/s	oreens/thaneset	.heml							💌 🛃 🐼
							Sag	Configuration Ping	Logout Befresh
CISCO	MONITOR	WLANS	CONTROLL	ER WJREI	LESS SECURITY	MANAGEMEN	COMMAN	DS HELP	
WLANs	WLANs.								New
* WLANS							Admin	_	
WLANS	Profile Nan	ne		Туре	WLAN SSED		Status	Security Policies	
Advanced	timeb			WLAN	tsweb		Enabled	[WPA2][Auth(802.1×)]	•
	Wired-Gutst			Guest LAN	Wired-Guest		Enabled	Web-Auth	

8. Ajoutez un utilisateur invité dans la base de données locale du contrôleur WLAN.

Cisco_48:53:c3 - Microsoft B	internet Explorer					X
File Edit View Favorites	Tools Help					J 🧤
🌀 Back + 🎲 - 💌 🙎] 🏠 🔎 Search 🤺 Favorites	- 🚱 🍰 😓 🗔 🛄 🛍 -				Links ¹⁰
Address () https://10.77.244.20	4/screens/frameset.html					💌 🔁 👳
					nfiguration Eing	Logout Refresh
cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local Net Users > Edit				< 8 ack	Apply
	User Name	guest				
General	Password	••••	J			
 RADIUS Authentication 	Confirm Password	••••				
Accounting	Lifetime (seconds)	86400	3			
▶ TACACS+	Guest User Role					
Local Net Users	Creation Time	Thu Nov 20 14:12:32 2008				
MAC Filtering Disabled Clients	Remaining Time	23 h 59 m 56 s				
User Login Policies	WLAN Profile	Wired-Guest				
E Local EAP	Description	Wired-guest				
Priority Order						
Access Control Lists						
Wireless Protection Policies						
▶ Web Auth						
▶ Advanced						
 Done 	-				🐴 🙂 3r	Lorret.
			, ,		" r	

Sur l'Étranger, vous devez définir l'entrée en tant que réseau local invité " configuré. " Vous devez associer la sortie à certaines interfaces, possiblement l'interface de gestion. Cependant, une fois le tunnel EoIP mis en place, le trafic est acheminé automatiquement par le tunnel plutôt que par l'adresse de gestion.

Accès par câble pour invité avec contrôleur d'ancrage WLAN

Dans cet exemple, l'adresse IP du contrôleur de réseau local sans fil à distance est 10.10.80.3 et l'adresse IP du contrôleur d'ancrage de zone démilitarisée (DMZ) est 10.10.75.2. Les deux font partie de groupes de mobilité différents.

1. Configurez le groupe de mobilité du contrôleur d'ancrage DMZ lorsque vous entrez l'adresse MAC, l'adresse IP et le nom du groupe de mobilité du contrôleur à distance.

and a hadron a								
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
CISCO Controller General Inventory Interfaces Multicast Network Routes Internal DHCP Server Mobility Management Mobility Groups Mobility Anchor Config	MONITOR Mobility (C This page al Mobility grou mobility grou address and spaces.	WLANS Group Me lows you to up member up member l group nam 04:b2:60 ea:a7:20	CONTROLLER embers > Edit o edit all mobility ; s are listed below is represented as ne(optional) separ	WIRELESS All group members , one per line. B s a MAC addres ated by one or bile-10	SECURITY at once. Each ss, IP more	MANAGEMENT	COMMANDS	HELP
Ports NTP > CDP > Advanced					Ŧ			

2. De même, configurez le groupe de mobilité du contrôleur à

distance.								
cisco		<u>W</u> LANs		R WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Controller	Mobility (Group Me	embers > Ed	it All				
General Inventory Interfaces Multicast Network Routes	This page al Mobility gro mobility gro address and spaces. 00:18:b9:0 00:18:73:	llows you to up member up member d group nan ea: a7:20 34: b2:60	o edit all mobility s are listed belo is represented ne(optional) sep 10.10.80.3 10.10.75.2	y group member w, one per line. as a MAC addre arated by one or acbile-9	s at once. Each ss, IP more			
Mobility Management Mobility Groups Mobility Anchor Config Ports NTP					<u>v</u>			
▶ CDP								
Advanced								

3. Créez le réseau WLAN câblé en lui donnant le même nom que le contrôleur WLAN d'ancrage. Dans ce cas, l'interface d'entrée n'est " aucune " car, logiquement, l'interface d'entrée est le tunnel EoIP à partir du contrôleur distant. L'interface de sortie est une interface différente, à laquelle les clients connectés par câble accèdent pour obtenir une adresse IP. Dans cet exemple, une interface dynamique appelée « guest » (invité) est créée. Cependant, à cette étape, vous ne pouvez pas activer le réseau WLAN puisqu'un message d'erreur s'affiche pour rappeler qu'une interface d'entrée ne peut pas indiquer « none » (aucun).



4. Sous « Security » (sécurité), configurez l'option « Layer 3 » (couche 3) selon le mode *web authentication* (authentification Web), de façon semblable au contrôleur à

distance.		
cisco	Rioratos Rinvar Contacites Albertas Becrato Managueria Comunes Helb.	Tugot Brinn
WLANS WLANS WLANS F Advanced	WLANE>EdR Cask General Security Gost Advanced Laper 2 Laper 3 Add Security Interferences Layer 3 Made Security Free Authentication Coll Free Authentication Coll Over rele Saled Config Exade	Apply

5. Créez l'ancrage de mobilité sur le contrôleur d'ancrage, puis associez-le à luimême.

								or Conferences Disc Learnet Balteria
CISCO	HONTON MLANE COM	TROLLER HUR	ELESS SECONTY	NAMENENT CONNUM	5 HU			
WLANs	WLANs							New
* WLANS	Profile Name	Туре	WLAN SSID	Admin Status	Security Policies			
NLAS-	al.	Windless	φ8	Enabled	Web-Auth	•		
* Advanced	<u>a</u>	Wireless	9 2	Enobled	Web-Auth			
	al	Windless	q3	Disabled	Web-Auth			
	week.cost	Wined	wined-gaset.	Enabled	Web-Auth	Factors		
						and the second		
and the local diversion of the local diversio								
CISCO	BORLIDE MARE COR	TROLLER W/F	ELESS SECURITY	HERRICEMENT COMMIN	ic Hela			
WLANs	Nobility Anchore							< Mack
- WLANS	MLAN SSID Hired-gu	61						
h Advanced	South IP Address (Ancho	-1				Data Path	Control Path	
· Morence	local					1.0	uş.	
	Nabidity Arachae Cree	de						
	Switch IP Address (And	hor)	10.39.50.3 9					

6. Après avoir créé l'ancrage de mobilité, retournez activer le réseau WLAN câblé.

uhuhu cisco	MONITOR WLANS O	ONTROLLER WIRELESS	SECURITY MAN	Saye IAGEMENT COMMANE	Configuration Ping DS HELP	Logout <u>R</u> efresh
WLANS WLANS WLANS MUANS	WLANs > Edit General Security Profile Name Type SSID Status	QoS Advanced wired-guest-1 Guest LAN wired-guest-1 R Enabled			< Back	Αρρίγ
	Security Policies Ingress Interface Egress Interface	Web-Auth (Modifications done unde None 💌 guest 💌	r security tab will app	pear after applying the d	hanges.)	

7. De même, créez l'ancrage de mobilité sur le contrôleur WLAN à distance pour le réseau WLAN par câble pour

/LANs	WLANs						New
* WLANS N(2A) F Advanced	Profile Name	Type	WLAN SSID	Admin Status	Security Policies		
	at.	Wireless	ph.	Enabled	Web-Auth		
	a2	Windless	92	Enabled	Web-Auth		
	41	Wireless	¢3	Disabled	Web-Auth		
	sinclused.	Wined	wired-guest.	Exobled	Web-Auth	Fathers	
						mage	
						and a	

Choisissez l'adresse IP du contrôleur WLAN d'ancrage, puis créez l'ancrage de mobilité.

cisco	ROFILLER WINNE CONTROLLER WEREESE RECIPULA HAVEEMENT COMMANDE HETS		any conjuntan (563) s	agent Extents
WLANs	Nobility Anchora			c mack
* WLANS	WLAN SSID wind-quart			
+ Advanced	Weitch IP Address (Anchor)	Data Path	Control Fath	
	20.18.78.2	up	ωp	
	Probibility Anchor Create			
	Switch IP Address (Anchor) 18.33.88.3(conf) 8			

Vérifiez si les données et la chaîne de commande sont opérationnelles. Si ce n'est pas le cas, assurez-vous que les ports suivants sont ouverts entre le contrôleur d'ancrage et le contrôleur de réseau local sans fil à distance : UDP 16666 ou IP 97.

8. Lorsque l'utilisateur invité est connecté par câble au commutateur et que l'authentification Web est terminée, le champ Policy Manager State (état du gestionnaire de politique) doit indiquer « RUN » et le champ Mobility Role (rôle de mobilité) doit indiquer « Export Foreign ».

cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY	MANAGEMENT COMM	ie <u>v</u> e Configuration <u>P</u> ing Logout <u>B</u> efrei MNDS HELP
Monitor Summary	Clients > Detail		< Back	Apply Link Test Remove
Access Points Statistics CDP	MAC Address IP Address Client Type	00:0d:60:5e:ca:62 0.0.0.0 Regular	AP Address AP Name AP Type	Unknown N/A Unknown
Clients Multicast	User Name Port Number Interface	1 110	WLAN Profile Status Association ID	wired-guest-1 Associated 0
	VLAN ID CCX Version E2E Version	110 Not Supported Not Supported	802.11 Authentication Reason Code Status Code	Open System 0 0
	Nobility Role Nobility Peer IP Address Policy Manager State	Export Foreign 10.10.75.2 RUN	CF Pollable CF Poll Request Short Preamble	Not Implemented Not Implemented Not Implemented
	Nirror Mode Nanagement Frame Protection	Disable 💌	PBCC Channel Agility	Not Implemented

De même, vérifiez l'état du contrôleur WLAN d'ancrage. Le champ Policy Manager State (état du gestionnaire de politique) doit indiquer « RUN » et le champ Mobility Role (rôle de mobilité) doit indiquer « Export

Save Configuration | Ping | Logout | Refr

Anchor ». ախտիս

CISCO	MONTION WDANS CONTR	OLLER WIRELESS SECORITY	MANAGEMENT COMM	ANUS HELP
Monitor	Clients > Detail		< Back	Apply Link Test Remove
Summary	Client Properties		AP Properties	
 Access Points 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
P COP	Client Type	Regular	AP Type	Mobile
P Rogues 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

Configuration par câble du client invité

Le client invité par câble reçoit une adresse IP du réseau VLAN de sortie, mais n'a pas accès au trafic avant de terminer le processus d'authentification Web.

Afin de vous connecter tant qu'utilisateur invité, procédez comme suit :

1. Ouvrez une fenêtre du navigateur Web et entrez l'URL souhaitée (par exemple, www.cisco.com). Vous serez redirigé vers la page Web par défaut du contrôleur de réseau local sans fil si l'authentification Web est activée, et la résolution DNS sera alors lancée pour l'URL entrée. Autrement, entrez l'URL suivante : https://1.1.1.1/login.html (l'adresse IP 1.1.1.1 correspond à l'adresse IP virtuelle du contrôleur de réseau local sans

fil).	
D Web Authentication - Microsoft Internet Explorer	() () () () () () () () () ()
File Edit View Favorites Tools Help	A *
🕝 Back - 🜍 - 🗷 🗟 🏠 🔎 Search 👷 Favorites 🤣 🎯 - 🌺 📼 🦓 💷 🛯	
Address 🕘 https://1.1.1.1/login.html 😒 🔁 😡	Linis 🎽 🥌 Snegit 🛐 📷
Google 🕞 🔹 📝 Go o 🧭 💆 👻 😭 Bookmarks 🛛 🐉 Oblocked 🛛 🎔 Check. 🖛 🔨 Autochik. 👻 🔚 Autorial 🖨 Send to 🕶 🥖	🔘 Settings 🕶
Login	
Welcome to the Cisco wireless network	
Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.	
User Name guest1	
Password ••••••	
Submit	
a Done	🖉 🌒 Internet

- 2. Entrez le nom d'utilisateur et le mot de passe fournis.
- 3. Lorsque la connexion est établie, une fenêtre s'affiche dans le navigateur Web.



Dépannage de la connexion par câble pour invité sur un contrôleur WLAN local

Ce processus de débogage contient tous les renseignements utiles concernant la connexion par câble d'un client invité.

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)

debug client

```
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
        op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
  DHCP
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
  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
  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
  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
   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
  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 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
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- <u>Configuration de la mobilité d'ancrage automatique</u>
- Exemple de configuration d'un WLAN invité et d'un WLAN interne à l'aide de contrôleurs de réseau local sans fil (WLC)
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil

- Guide de configuration du contrôleur de réseau local sans fil Cisco, version 4.2
- <u>Assistance produit sans fil</u>
- Support et documentation techniques Cisco Systems

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.