رسجل ةددعتملا VLAN ةكبش معد نيوكت (WGB) لمعلا ةعومجم

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة التكوين WGB مع شبكات VLAN متعددة مرتبطة بنقطة الوصول CAPWAP الرسم التخطيطي للشبكة تكوين وحدة التحكّم في شبكة LAN اللاسلكية (WLC). تهىئة WGB <u>تكوين المبدّل</u> <u>WGB مع محول 802.1g متأخر وشبكات VLAN متعددة مرتبطة بنقطة وصول مستقلة في الوضع الجذر.</u> الرسم التخطيطي للشبكة تكوين نقطة الوصول الجذر تهىئة WGB تكوين المبدّل <u>WGB بدون محول خلف وشبكات VLAN متعددة مرتبطة بنقطة وصول مستقلة في الوضع الجذر.</u> <u>الرسم التخطيطي للشبكة</u> تكوين نقطة الوصول الجذر تهيئة WGB <u>التحقق من</u> الصحة

المقدمة

يشرح هذا المستند كيفية تكوين WGB لدعم شبكات المنطقة المحلية الظاهرية المتعددة (VLANs) تحت سيناريوهات مختلفة.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة أساسية في AireOS لاسلكي lan جهاز تحكم (WLC) ونقطة الوصول (AP) في أسلوب تشكيل مستقل.

المكونات المستخدمة

- WLC الإصدار 8.2
- نقطة الوصول المستقلة V15.3(3)JD4
- التحكم في نقطة الوصول (CAPWAP) اللاسلكية وإمدادها

• إمكانية المحول 802.1<mark>q</mark>

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

التكوين

WGB مع شبكات VLAN متعددة مرتبطة بنقطة الوصول CAPWAP

يشرح هذا المثال كيفية تكوين WGB يدعم شبكات VLAN متعددة، مقترنة بنقطة وصول CAPWAP. يمكن أن تكون نقطة الوصول في الوضع المحلي أو في وضع الجسر (شبكة). يتطلب هذا السيناريو أن تكون WGB متصلة بمحول يدعم 802.1q، وإلا فإن WGB لا تدعم شبكات VLAN متعددة. في هذا المثال، يتم توصيل WGB بمحول Cisco 3560.

إن لا يساند المفتاح VLAN أهلي طبيعي. إن لا يساند المفتاح VLAN أهلي طبيعي.

في هذا المثال، يتم تخصيص WGB لشبكة VLAN رقم 210 ويتم تخصيص العملاء المتصلين بالمحول خلف شبكة WGB لشبكة VLAN رقم 2601 و 2602.

ال WLC ينبغي أيضا يتلقى شكلت قارن حركي أن ينتسب إلى الزبون VLAN. في هذا مثال ال WLC ينبغي يتلقى داينانيك قارن على 2602، 2601 و 210.

الرسم التخطيطي للشبكة



تكوين وحدة التحكّم في شبكة LAN اللاسلكية (WLC)

الخطوة 1. افتح واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وتصفح إلى **وحدة التحكم > الواجهات** للتحقق من الواجهات الديناميكية الحالية التي تم تكوينها على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC).إذا لم يتم تكوين شبكات VLAN المطلوبة بالفعل، فانقر فوق **جديد** وأضف الشبكات المطلوبة.

սիսիս							Save Configuration Ping	Logout <u>R</u> efres
CISCO	MONITOR WLANS CONTROLLER	WIRELESS	SECURITY MANA	Gement C <u>o</u> mi	1ANDS HELP <u>F</u> EEDBAC	к		n <u>H</u> ome
Controller	Interfaces						Entries 1 - 3 of	3 New
General								
Icons	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address		
Inventory	management	2601	172.:	Static	Enabled	2001:		
Interfaces	virtual	N/A	192.0.2.1	Static	Not Supported			
Interface Groups	<u>v: 2000</u>	2		Dynamic	Disabled			

alaha sa							Sa <u>v</u> e Cor	figuratio	n <u>P</u> ing Lo	gout <u>R</u> efresh
cisco	MONITOR V	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	n <u>H</u> ome
Controller	Interfaces >	> New							< Back	Apply
General	Interface Na	ame v	lan210							
Icons	VI AN Id		10							
Inventory										
Interfaces										
Interface Groups										

إدخال معلومات الواجهة

< Back Apply

Interfaces > Edit

General Information

Interface Name	vlan210
MAC Address	80:e8:6f:02:6a:60

Configuration

Guest Lan	
Quarantine	
Quarantine Vlan Id	0
NAS-ID	none

Physical Information

Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Managemen	t 🔲

Interface Address

VLAN Identifier	210		
IP Address	ip-addr		
Netmask	net-mask		
Gateway	gw		
OHCP Information			
Primary DHCP Server		optional-dh	ср
Secondary DHCP Server			

ملاحظة: إذا كان عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لديك تم تمكين تجميع الارتباطات (LAG)، فلن تتمكن من تحديد رقم منفذ.

الخطوة 2. انتقل إلى **شبكات WLAN > إنشاء جديد > انتقال.**

،، ،،، ،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK							
WLANs	WLANs							
WLANS WLANS WLANS Advanced	Current Filter: None [Change Filter] [Clear Filter] Create New Create New							

الخطوة 3. أختر اسما لمعرف SSID والتوصيف، ثم انقر على **تطبيق.**

Ν	/LANs > New			< Back	Apply
	Туре	WLAN V			
	Profile Name	profile-name			
	SSID	SSID-name			
	ID	2 ~	•		

:CLI

> config wlan create <id> <profile-name> <ssid-name</p>الخطوة 4. عينت ال WGB أهلي طبيعي VLAN إلى ال

MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP F
WLANs >	Edit 'v	/gb-tst'					< E
General	Secu	rity QoS	Policy-Map	ping Adv	vanced		
Profile	Name	wgb	-tst				
Туре		WLA	N				
SSID		wgb	-tst				
Status			nabled				
Securit	y Policies	[WI (Mod	PA2][Auth(802 ifications done u	2.1X)] under security t	ab will appear afte	er applying the cha	inges.)
Radio P	Policy	All	\$				
Interfac	ce/Interfac	e 🖂	-210				

الخطوة 5. قم بتعيين المفتاح المشترك مسبقا الذي يستخدمه WGB لإقرانه بمعرف SSID.

انتقل إلى **الأمان > الطبقة 2 > إدارة مفتاح المصادقة.** حدد PSK وقم بتعبئة كلمة المرور.

،، ،،، ،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'wgb-tst'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers PMF Disabled \$
	WPA+WPA2 Parameters
	WPA Policy WPA2 Policy
	WPA2 Encryption AES TKIP
	OSEN Policy Authentication Key Management 12
	802.1X Enable
	PSK PSK
	FT 802.1X Enable FT PSK Enable
	PSK Format ASCII \$
	WPA gtk-randomize State Disable \$

الخطوة 6. تأكد من أن الشبكة المحلية اللاسلكية (WLAN) لديها تمكين Aironet IE، وإلا فلن يتمكن WGB من الاقتران.

WLANs > Edit 'wgb-tst'

General	Security	QoS	Policy-Mapping	Advanced	
Allow AA	A Override		Enabled		DHCP
Coverag	e Hole Detectior	n	Enabled		DHCP
Enable S	Session Timeout				
Aironet	ΙE		🕑 Enabled		DHCP .
Diagnos	tic Channel ¹⁸		Enabled		OEAP
Override	Interface ACL		IPv4 None 🗘	IPv6 No	ne 🗘 Split T
Layer2 A	Acl		None \$		

ملاحظة: في هذا المثال، تستخدم SSID تأمين WPA2/PSK، إذا احتجت إلى تكوين شبكة WLAN بأسلوب تأمين أقوى مثل WPA2/802. 1x يمكنك مراجعة هذا الارتباط: <u>مصادقة 1x 802 مع PEAP، ISE 2. 1 و</u> <u>WLC 8. 3</u>

الخطوة 7. مكنت ال WLC أن يساند يتعدد VLANs من WGB

config wgb vlan enable<

تهيئة WGB

الخطوة 1. قم بإضافة الواجهات الفرعية المطلوبة لكل شبكة VLAN. في هذا المثال، تتم إضافة شبكات VLAN رقم 210 (أصلي) و 2601 و 2602 إلى تكوين WGB.

WGB# config t WGB# interface dotllradio 0.210 WGB# encapsulation dotlq 210 native

WGB# interface dotllradio 0.2601 WGB# encapsulation dotlq 2601 WGB# bridge-group 21

WGB# interface dotllradio 0.2602 WGB# encapsulation dotlq 2602 WGB# bridge-group 22

WGB# interface dot11radio 1.210 WGB# encapsulation dot1q 210 native

WGB# interface dotllradio 1.2601 WGB# encapsulation dotlq 2601 WGB# bridge-group 21

WGB# interface dotllradio 1.2602 WGB# encapsulation dotlq 2602 WGB# bridge-group 22

WGB# interface gigabit 0.210 WGB# encapsulation dot1q 210 native

> WGB# interface gigabit 0.2601 WGB# encapsulation dot1q 2601 WGB# bridge-group 21

> WGB# interface gigabit 0.2602 WGB# encapsulation dot1q 2602 WGB# bridge-group 22

ملاحظة: مجموعة جسور من الواجهات الفرعية 2601 و 2602 هي 21 و 22 لأن النطاق الصحيح لمجموعات الجسر هو من 1 إلى 255.

ملاحظة: لم يتم تحديد مجموعة جسور للواجهة الفرعية 210 لأنه عندما يتم تعيين شبكة VLAN الأصلية إلى واجهة فرعية، فإنها تقوم تلقائيا بتعيين مجموعة الجسر 1.

الخطوة 2. قم بإنشاء معرف مجموعة الخدمة (SSID).

في هذا المثال تستخدم SSID WPA2/PSK، إذا احتجت إلى WGB للاقتران ب SSID بأسلوب تأمين أقوى مثل WPA2/802. 1x يمكنك مراجعة هذا الرابط:

جسور مجموعة العمل مع تشكيل مصادقة PEAP مثال

WGB# config t WGB# dot11 ssid wgb-tst WGB# dot11 ssid wgb-tst WGB# vlan 210 WGB# authentication open WGB# authentication key-management wpa version 2 WGB# infrastructure-ssid WGB# infrastructure-ssid WGB# wpa-psk ascii 0 ciscol23 Itخطوة 3. قم بإضافة SSID في الواجهة المستخدمة للاقتران بنقطة الوصول CAPWAP. كما أدت هذه الخطوة إلى تعيين نقطة الوصول كجسر مجموعة العمل باستخدام الأمر **-station-role workgroup** bridge.

ملاحظة: في هذا المثال، تستخدم واجهة WGB الخاصة بها بسرعة 2.4 جيجاهرتز للاقتران بنقطة الوصول CAPWAP، إذا كنت بحاجة إلى نقطة الوصول WGB للاقتران بواجهة 5 جيجاهرتز الخاصة بها، فقم بإضافة هذا التكوين إلى الواجهة dot11Radio1.

> WGB# config t WGB# interface DotllRadio0 WGB# encryption vlan 210 mode ciphers aes-ccmp WGB# ssid WGB-tst WGB# station-role workgroup-bridge

> > الخطوة 4. مكنت ال WGB unified VLAN سمة.

سيسمح هذا أمر ال WGB أن يعلم ال WLC في أي VLAN الزبون ينبغي عينت.

WGB# config t WGB# workgroup-bridge unified-vlan-client

تكوين المبدّل

الخطوة 1. قم بإنشاء شبكات VLAN.

S₩# config t S₩# vlan 210, 2601, 2602 الخطوة 2. قم بتكوين المنفذ الذي يتم فيه توصيل WGB.

SW# config t <SW# interface <interface-id SW# switchport mode trunk SW# switchport trunk native vlan 210 SW# switchport trunk allowed vlan 210, 2601, 2602 الخطوة 3. عينت القارن حيث الزبون يكون ربطت إلى ال يحتاج VLAN.

> SW# config t <SW# interface <interface-id SW# switchport mode access <SW# switchport access vlan <vlan-id

WGB مع محول 802.1q متأخر وشبكات VLAN متعددة مرتبطة بنقطة وصول مستقلة في الوضع الجذر.

الرسم التخطيطي للشبكة



تكوين نقطة الوصول الجذر

الخطوة 1. قم بإضافة الواجهات الفرعية المطلوبة لكل شبكة VLAN.

في هذا المثال، تتم إضافة شبكات VLAN رقم 210 (أصلي) و 2601 و 2602 إلى تكوين نقطة الوصول عن طريق الجذر كما هو موضح في الخطوة 1 من <u>WGB مع شبكات VLAN متعددة مقترنة بنقطة الوصول CAPWAP - تكوين</u>. <u>WGB.</u>

الخطوة 2. قم بإنشاء معرف مجموعة الخدمة (SSID).

في هذا المثال، يستخدم SSID WPA2/PSK، إذا احتجت إلى تكوين نقطة الوصول الجذر باستخدام SSID باستخدام طريقة تأمين أقوى مثل WPA2/802.1x يمكنك مراجعة هذا الرابط:

<u>تكوين معرّفات SSID وشبكات VLAN على نقاط الوصول الذاتية</u>

Root-AP# config t Root-AP# dot11 ssid WGB-tst Root-AP# vlan 210 Root-AP# authentication open Root-AP# authentication key-management wpa version 2 Root-AP# infrastructure-ssid Root-AP# wpa-psk ascii 0 cisco123

الخطوة 3. قم بإضافة SSID إلى الواجهة التي ستستخدمها نقطة الوصول الجذر لبث SSID.

ملاحظة: في هذا المثال، تستخدم نقطة الوصول (AP) الجذر واجهة بسرعة 2.4 جيجاهرتز الخاصة بها لبث SSID، إذا كنت بحاجة إلى نقطة الوصول (AP) الجذر لبثها باستخدام واجهة بسرعة 5 جيجاهرتز، فقم بإضافة هذا التكوين إلى الواجهة Dot11Radio1.

> Root-AP# config t Root-AP# interface DotllRadioO Root-AP# encryption vlan 210 mode ciphers aes-ccmp Root-AP# ssid WGB-tst Root-AP# infrastructure-client Root-AP# no shut

يسمح الأمر **infrastructure-client** لنقطة الوصول الجذر باحترام تعيين شبكة VLAN الذي توفره WGB لعملائها السلكيين. بدون هذا الأمر، ستعين نقطة الوصول الجذر جميع العملاء لشبكة VLAN الأصلية.

تهيئة WGB

الخطوة 1. قم بإضافة الواجهات الفرعية المطلوبة لكل شبكة VLAN.

في هذا المثال، تتم إضافة شبكات VLAN رقم 210 (أصلي) و 2601 و 2602 إلى تكوين نقطة الوصول عن طريق الجذر كما هو موضح في الخطوة 1 من <u>WGB مع شبكات VLAN متعددة مقترنة بنقطة الوصول CAPWAP - تكوين</u>. <u>WGB.</u>

الخطوة 2. قم بإنشاء معرف مجموعة الخدمة (SSID).

في هذا المثال تستخدم SSID WPA2/PSK، إذا احتجت إلى WGB للاقتران ب SSID بأسلوب تأمين أقوى مثل WPA2/802. 1x يمكنك مراجعة هذا الرابط:

<u>جسور مجموعة العمل مع تشكيل مصادقة PEAP مثال</u>

WGB# config t WGB# dotll ssid WGB-tst WGB# vlan 210 WGB# authentication open WGB# authentication key-management wpa version 2 WGB# infrastructure-ssid WGB# infrastructure-ssid WGB# wpa-psk ascii 0 ciscol23 الخطوة 3. قم بإضافة SSID في الواجهة المستخدمة للاقتران بنقطة الوصول CAPWAP.

كما أدت هذه الخطوة إلى تعيين نقطة الوصول كجسر مجموعة العمل باستخدام الأمر **-station-role workgroup** bridge.

ملاحظة: في هذا المثال، تستخدم واجهة WGB الخاصة بها بسرعة 2.4 جيجاهرتز للاقتران بنقطة الوصول CAPWAP، إذا كنت بحاجة إلى نقطة الوصول WGB للاقتران بواجهة 5 جيجاهرتز الخاصة بها، فقم بإضافة هذا التكوين إلى الواجهة dot11Radio1.

> WGB# config t WGB# interface Dotl1Radio0 WGB# encryption vlan 210 mode ciphers aes-ccmp WGB# ssid WGB-tst WGB# station-role workgroup-bridge WGB# no shut

تكوين المبدّل

يمكنك اتباع نفس التكوين للمحول على <u>WGB مع شبكات VLAN متعددة مقترنة بنقطة الوصول CAPWAP.</u>

WGB بدون محول خلف وشبكات VLAN متعددة مرتبطة بنقطة وصول مستقلة في الوضع الجذر.

يسمح هذا مثال WGB أن يستعمل VLANs 2 مختلف (أهلي طبيعي وآخر)، إن يحتاج أنت أن يتلقى أكثر من إثنان VLANs بعد ذلك أنت تحتاج أن يضيف 802.1Q مفتاح قادر خلف WGB ويربط الزبون عليه. ثم اتبع التعليمات الموجودة على <u>WGB مع وجود محول 802.1Q خلف وشبكات VLAN متعددة مرتبطة بنقطة وصول (AP) مستقلة</u> <u>في الوضع الجذر</u>.



تكوين نقطة الوصول الجذر

الخطوة 1. قم بإضافة الواجهات الفرعية المطلوبة لكل شبكة VLAN.

يكون تكوين الواجهات الفرعية هو نفسه كما يرى على الخطوة 1 من <u>WGB مع شبكات VLAN المتعددة المقترنة</u> <u>بنقطة الوصول CAPWAP - تكوين WGB</u>، ولكن في هذه الحالة تحتاج فقط إلى تكوين شبكة VLAN 210 (أصلي) وشبكة VLAN 2602 (عميل VLAN).

الخطوة 2. قم بإنشاء معرف مجموعة الخدمة (SSID).

في هذا المثال، يستخدم SSID WPA2/PSK، إذا احتجت إلى تكوين نقطة الوصول الجذر باستخدام SSID باستخدام طريقة تأمين أقوى مثل WPA2/802.1x يمكنك مراجعة هذا الرابط:

<u>تكوين معرّفات SSID وشبكات VLAN على نقاط الوصول الذاتية</u>

Root-AP# config t Root-AP# dot11 ssid WGB-tst Root-AP# vlan 210 Root-AP# authentication open Root-AP# authentication key-management wpa version 2 Root-AP# infrastructure-ssid Root-AP# wpa-psk ascii 0 cisco123

الخطوة 3. قم بإضافة SSID إلى الواجهة التي ستستخدمها نقطة الوصول الجذر لبث SSID.

ملاحظة: في هذا المثال، تستخدم نقطة الوصول (AP) الجذر واجهة بسرعة 2.4 جيجاهرتز الخاصة بها لبث SSID، إذا كنت بحاجة إلى نقطة الوصول (AP) الجذر لبثها باستخدام واجهة بسرعة 5 جيجاهرتز، فقم بإضافة هذا التكوين إلى الواجهة Dot11Radio1.

Root-AP# config t Root-AP# interface Dot11Radio0 Root-AP# encryption vlan 210 mode ciphers aes-ccmp Root-AP# ssid WGB-tst Root-AP# infrastructure-client Root-AP# no shut الأمر **عميل البنية الأساسية** السماح لنقطة الوصول الجذر باحترام تعيين شبكة VLAN التي لدى WGB لعملائها السلكيين. بدون هذا الأمر، تعين نقطة الوصول الجذر جميع العملاء إلى شبكة VLAN الأصلية. الخطوة 1. قم بإضافة الواجهات الفرعية المطلوبة لكل شبكة VLAN. في هذا مثال أضفت VLANs 210 (أهلي طبيعي) و 2601 إلى ال WGB تشكيل.

تكوين الواجهات الفرعية هو نفسه كما يظهر على الخطوة 1 من <u>WGB مع شبكات VLAN متعددة مرتبطة بنقطة</u> <u>وصول CAPWAP - تكوين WGB</u>، غير أن في هذه الحالة يحتاج فقط أن يشكل VLAN 210 (أهلي طبيعي) و VLAN 2602 (زبون VLAN).

الخطوة 2. قم بإنشاء معرف مجموعة الخدمة (SSID).

في هذا المثال تستخدم SSID WPA2/PSK، إذا احتجت إلى WGB للاقتران ب SSID بأسلوب تأمين أقوى مثل WPA2/802. 1x يمكنك مراجعة هذا الرابط:

<u>جسور مجموعة العمل مع تشكيل مصادقة PEAP مثال</u>

WGB# config t WGB# dotll ssid WGB-tst WGB# vlan 210 WGB# authentication open WGB# authentication key-management wpa version 2 WGB# infrastructure-ssid WGB# infrastructure-ssid WGB# wpa-psk ascii 0 ciscol23 Itخطوة 3. قم بإضافة SSID في الواجهة المستخدمة للاقتران بنقطة الوصول CAPWAP.

كما أدت هذه الخطوة إلى تعيين نقطة الوصول كجسر مجموعة العمل باستخدام الأمر **-station-role workgroup** bridge.

ملاحظة: في هذا المثال، تستخدم واجهة WGB الخاصة بها بسرعة 2.4 جيجاهرتز للاقتران بنقطة الوصول CAPWAP، إذا كنت بحاجة إلى نقطة الوصول WGB للاقتران بواجهة 5 جيجاهرتز الخاصة بها، فقم بإضافة هذا التكوين إلى الواجهة dot11Radio1.

> WGB# config t WGB# interface DotllRadio0 WGB# encryption vlan 210 mode ciphers aes-ccmp WGB# ssid WGB-tst WGB# station-role workgroup-bridge WGB# no shut

> > الخطوة 4. عينت الزبون VLAN.

WGB# workgroup-bridge client-vlan 2601

التحقق من الصحة

قم بتشغيل هذا الأمر للتحقق من أن WGB مرتبط بنقطة الوصول الجذر، وأن نقطة الوصول (AP) الجذر يمكنها رؤية العملاء المتصلين خلف WGB:

WGB# show dot11 associations

: [SSID [WGB-tst

MAC Address	IP address	IPV6	address	Device	Name
				Parent	State
00eb.d5ee.da70	200.200.200.4	::		ap1600-Parent	Root-AP
				-	Assoc

Root-AP# show dot11 associations

:Client Stations on Dot11Radio0 802.11

: [SSID [WGB-tst

MAC Address	IP address	IPV6 address	Device	Name	
			Parent	State	
0035.1ac1.78c7 206.206.206.2 ::			WGB-clie	WGB-client -	
			00f6.6316.425	3 Assoc	
00f6.6316.42	58 200.200.200.	3 ::	WGB	WGB	
			self	Assoc	

ةمجرتاا مذه لوح

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