# Configuration de l'affectation dynamique de VLAN avec NGWC et ACS 5.2

# Contenu

Introduction Conditions préalables **Conditions requises** Components Used Affectation de VLAN dynamique avec le serveur RADIUS Configuration Diagramme du réseau **Hypothèses** Configuration du WLC avec CLI **Configurer WLAN** Configurer le serveur RADIUS sur WLC Configurer le pool DHCP pour le VLAN client Configuration du WLC avec l'interface graphique utilisateur **Configurer WLAN** Configurer le serveur RADIUS sur WLC **Configurer le serveur RADIUS** Vérification Dépannage

# Introduction

Ce document décrit le concept d'affectation de VLAN dynamique. Il décrit également comment configurer le contrôleur de réseau local sans fil (WLC) et un serveur RADIUS afin d'affecter des clients de réseau local sans fil (WLAN) à un VLAN spécifique de manière dynamique. Dans ce document, le serveur RADIUS est un serveur de contrôle d'accès (ACS) qui exécute Cisco Secure Access Control System Version 5.2.

# Conditions préalables

## **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

• Connaissance de base du WLC et des points d'accès légers (LAP)

- Connaissance fonctionnelle du serveur AAA (Authentication, Authorization and Accounting)
- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil

## **Components Used**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil Cisco 5760 avec logiciel Cisco IOS<sup>®</sup> XE version 3.2.2 (armoire de câblage nouvelle génération ou NGWC)
- Point d'accès allégé de la gamme Cisco Aironet 3602
- Microsoft Windows XP avec Intel Proset Supplicator
- Cisco Secure Access Control System version 5.2
- Commutateur de la gamme Cisco Catalyst 3560

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.

# Affectation de VLAN dynamique avec le serveur RADIUS

Dans la plupart des systèmes WLAN, chaque WLAN a une stratégie statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier), ou WLAN dans la terminologie du contrôleur. Bien que puissante, cette méthode a des limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

Cependant, la solution WLAN de Cisco prend en charge la mise en réseau d'identités. Cela permet au réseau d'annoncer un SSID unique, mais permet à des utilisateurs spécifiques d'hériter de différentes QoS, attributs VLAN et/ou stratégies de sécurité en fonction des informations d'identification de l'utilisateur.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. Cette tâche d'affectation des utilisateurs à un VLAN spécifique est gérée par un serveur d'authentification RADIUS, tel qu'un Cisco Secure ACS. Cette fonctionnalité peut être utilisée, par exemple, afin de permettre à l'hôte sans fil de rester sur le même VLAN qu'il se déplace au sein d'un réseau de campus.

Par conséquent, lorsqu'un client tente de s'associer à un LAP enregistré auprès d'un contrôleur, le LAP transmet les informations d'identification de l'utilisateur au serveur RADIUS pour validation. Une fois que l'authentification est réussie, le serveur RADIUS passe certains attributs de l'Internet Engineering Task Force (IETF) à l'utilisateur. Ces attributs RADIUS décident de l'ID de VLAN qui doit être affecté au client sans fil. Le SSID du client (le WLAN, en termes de WLC) n'a pas d'importance car l'utilisateur est toujours affecté à cet ID de VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

- IETF 64 (Tunnel Type) : défini sur VLAN.
- IETF 65 (Tunnel Medium Type) : défini sur 802.
- IETF 81 (Tunnel-Private-Group-ID) Défini sur l'ID VLAN.

L'ID de VLAN est de 12 bits et prend une valeur comprise entre 1 et 4 094, inclus. Étant donné que l'ID de groupe privé-tunnel est de type chaîne, comme défini dans <u>RFC 2868, Attributs</u> <u>RADIUS pour la prise en charge du protocole de tunnel</u> pour utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée en tant que chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme observé dans RFC2868, section 3.1:

«Le champ Tag est d'un octet de longueur et est destiné à fournir un moyen de regrouper des attributs dans le même paquet qui font référence au même tunnel. »

Les valeurs valides pour le champ Tag sont 0x01 à 0x1F, inclusivement. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à RFC 2868 pour plus d'informations sur tous les attributs RADIUS.

# Configuration

La configuration d'une affectation de VLAN dynamique se compose de deux étapes distinctes :

- 1. Configurez le WLC à l'aide de l'interface de ligne de commande (CLI) ou de l'interface utilisateur graphique.
- 2. Configurez le serveur RADIUS.

Note: Utilisez l'<u>Outil de recherche de commande (clients inscrits seulement) pour obtenir</u> plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Ce document utilise 802.1X avec le protocole PEAP (Protected Extensible Authentication Protocol) comme mécanisme de sécurité.

## Hypothèses

- Les commutateurs sont configurés pour tous les VLAN de couche 3 (L3).
- Une étendue DHCP est attribuée au serveur DHCP.
- La connectivité de couche 3 existe entre tous les périphériques du réseau.
- Le LAP est déjà joint au WLC.
- Chaque VLAN a un masque /24.
- ACS 5.2 possède un certificat auto-signé installé.

## Configuration du WLC avec CLI

**Configurer WLAN** 

Voici un exemple de configuration d'un WLAN avec le SSID de DVA :

```
wlan DVA 3 DVA
aaa-override
client vlan VLAN0020
security dot1x authentication-list ACS
session-timeout 1800
no shutdown
```

#### Configurer le serveur RADIUS sur WLC

Voici un exemple de configuration du serveur RADIUS sur le WLC :

```
aaa new-model
!
!
aaa group server radius ACS
server name ACS
!
aaa authentication dot1x ACS group ACS
radius server ACS
address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
key Ciscol23
```

#### dot1x system-auth-control

#### Configurer le pool DHCP pour le VLAN client

Voici un exemple de configuration du pool DHCP pour les VLAN 30 et 40 du client :

```
interface Vlan30
ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
ip address 40.40.40.1 255.255.255.0
ip dhcp pool vla30
network 30.30.30.0 255.255.255.0
default-router 30.30.30.1
!
ip dhcp pool vlan40
network 40.40.40.0 255.255.255.0
default-router 40.40.40.1
ip dhcp snooping vlan 30,40
ip dhcp snooping
```

# Configuration du WLC avec l'interface graphique utilisateur

#### **Configurer WLAN**

Cette procédure décrit comment configurer le WLAN.

1. Accédez à Configuration > Wireless > WLAN > NEW tab.

.1	linin isco w	/ireless Con	troller				
	😚 Home	Monitor 🛛 🔻	Configuration 💌	Ac	ministration		
<b>Wireless</b> • WLAN			Wizard Controller	L <b>ANs</b> Mobility Anchor			
							UWLANs
► A ► 8	ccess Points 02.11a/n		Commands		wpa2psk		
▶ 802 11b/o/n							

2. Cliquez sur l'onglet **General** afin de voir que le WLAN est configuré pour WPA2-802.1X et mappez l'interface/groupe d'interfaces(G) au VLAN 20 (**VLAN0020**).

WLAN > Edit							
General Security QOS	Advanced						
Profile Name	DVA						
Туре	WLAN						
SSID	DVA						
Status							
Security Policies	[WPA2][Auth(802.1x)] (Modifications done under security tab will appear after applying the changes.)						
Radio Policy	All 👻						
Interface/Interface Group(G)	VLAN0020 -						
Broadcast SSID							
Multicast VLAN Feature							

3. Cliquez sur l'onglet **Avancé** et cochez la case **Autoriser le remplacement AAA**. La substitution doit être activée pour que cette fonctionnalité fonctionne.

WLAN > Edit						
General	Security	QOS	Advanced			
Allow AAA Override 🗹 Coverage Hole Detection 🗹						
Session Timeout (secs) 1800						

4. Cliquez sur l'onglet **Security** et l'onglet **Layer2**, cochez la case WPA2 Encryption **AES**, puis sélectionnez **802.1x** dans la liste déroulante Auth Key Mgmt.

WLAN > Edit							
General Security QOS Advanced							
Layer2 Layer3 AAA Server							
Layer 2 Security WPA + WPA2 💌							
MAC Filtering							
WPA Policy  WPA2 Parameters WPA2 Policy  WPA2 Policy  AES  TKIP							
Auth Key Mgmt 802.1x 👻							

## Configurer le serveur RADIUS sur WLC

Cette procédure décrit comment configurer le serveur RADIUS sur le WLC.

1. Accédez à l'onglet Configuration > Sécurité.

cisco Wireless Cont	troller	
🏠 Home Monitor 🔻	Configuration 💌	Administration
<ul> <li>AAA</li> <li>Method Lists</li> <li>General</li> <li>Authentication</li> </ul>	Wizard Controller Wireless <u>Security</u> Commands	eneral Local Authenti Local Authoriza
<ul> <li>Accounting</li> <li>Authorization</li> <li>Server Groups</li> </ul>		

2. Accédez à **AAA** > **Groupes de serveurs** > **Radius** afin de créer les groupes de serveurs Radius. Dans cet exemple, le groupe de serveurs Radius est appelé ACS.

☆ Home Monitor : ▼ Configuration : ▼	Administration : 🔻 Help						
ecurity	Radius Server Groups						
AAA	New Remove						
<ul> <li>Method Lists</li> </ul>	Name	Server1	Server2	Server3			
General							
Authentication	ACS	ACS	N/A	N/A			
Accounting							
Authorization							
▼ Server Groups							
😐 Radius							

3. Modifiez l'entrée Radius Server afin d'ajouter l'adresse IP du serveur et le secret partagé. Ce secret partagé doit correspondre au secret partagé sur le WLC et le serveur RADIUS.

cisco Wireless Controller			
🏠 Home Monitor 🛛 Configuration 🖓 🔻	Administration 💌 Help		
Security	Radius Servers Radius Servers > Edit		
<ul> <li>Method Lists</li> <li>General</li> </ul>	Server Name Server IP Address	ACS 10.106.102.50	
<ul> <li>Authentication</li> <li>Accounting</li> </ul>	Shared Secret Confirm Shared Secret	••••••	
<ul> <li>Authorization</li> <li>Server Groups</li> <li>Badius</li> </ul>	Acct Port (0-65535) Auth Port (0-65535)	1645	
<ul> <li>Tacacs+</li> <li>Ldap</li> </ul>	Server Timeout (0-1000) secs Retry Count (0-100)		
▼ RADIUS			

Voici un exemple de configuration complète :

Radius Servers							
New Remove							
Server Name	Address	Auth Port	Acct Port				
ACS	10.106.102.50	1645	1646				

## Configurer le serveur RADIUS

Cette procédure décrit comment configurer le serveur RADIUS.

- 1. Sur le serveur RADIUS, accédez à Utilisateurs et magasins d'identités > Magasins d'identités internes > Utilisateurs.
- 2. Créez les noms d'utilisateur et les groupes d'identités appropriés. Dans cet exemple, il s'agit de Student et All Groups:Students, et Teacher et AllGroups:Teachers.



3. Accédez à Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles et créez les profils d'autorisation pour AAA override.

🕨 🚭 My Workspace	Policy Bements > Authorization and Permissions > Network Access > Authorization F						
Network Resources	Author	Authorization Profiles					
Users and Identity Stores	Filter:		Match if Go 🔻	-			
🔹 🦻 Policy Elements							
<ul> <li>Session Conditions</li> </ul>		Name 🔺	Description				
Date and Time		Permit Access					
Custom		Student	Student				
Authorization and Permissions		teacher	teacher				
<ul> <li>Network Access         <ul> <li>Authorization Profiles</li> <li>Device Administration</li> <li>Named Permission Objects</li> </ul> </li> </ul>							
Access Policies							

4. Modifiez le profil d'autorisation de l'étudiant.



5. Définissez l'ID/nom du VLAN comme Statique avec une valeur de 30 (VLAN 30).

Pol	icy Elements > Authorization and F	Permissions > Ne	tw o	rk Access > Authorization Profiles > Edit: "Student"
Γ	General Common Tasks	RADIUS Attri	oute	es
L	ACLS		_	
L	Downloadable ACL Name:	Not in Use	•	
L	Filter-ID ACL:	Not in Use	•	
L	Proxy ACL:	Not in Use	•	
L	Voice VLAN			
L	Permission to Join:	Not in Use	•	
L	VLAN			
L	VLAN ID/Name:	Static	•	Value 30
L	Reauthentication			
L	Reauthentication Timer:	Not in Use	•	
l	Maintain Connectivity during Reauthentication: QOS			
L	Input Policy Map:	Not in Use	•	
L	Output Policy Map:	Not in Use	•	
L	802.1X-REV			
L	LinkSec Security Policy:	Not in Use	•	
L	URL Redirect			
L	When a URL is defined for R	edirect an ACL	nus	stalso be defined
	URL for Redirect:	Not in Use	•	
	URL Redirect ACL:	Not in Use	Ŧ	
	= Required fields			

6. Modifiez le profil d'autorisation de l'enseignant.

Pol	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "teacher"								
	General Com	nmon Tasks	RADIUS Attributes						
	🌣 Name:	teacher							
	Description:	teacher							
	♥ = Required fields								

7. Définissez l'ID/nom du VLAN comme Statique avec une valeur de 40 (VLAN 40).

Poli	cy Elements > Authorization and F	Permissions > Netw	ork Access > Authorization Profiles > Edit: "teacher"
	General Common Tasks	RADIUS Attribu	ites
	ACLS	n.	
	Downloadable ACL Name:	Not in Use 🛛 👻	
	Filter-ID ACL:	Not in Use 🔹	
	Proxy ACL:	Not in Use 🛛 👻	
	Voice VLAN		
	Permission to Join:	Not in Use 🛛 👻	
	VLAN		
	VLAN ID/Name:	Static -	🗢 Value 40
	Reauthentication		
	Reauthentication Timer:	Not in Use 🛛 👻	
	Maintain Connectivity during Reauthentication: QOS		
	Input Policy Map:	Not in Use 🛛 👻	
	Output Policy Map:	Not in Use 🛛 👻	
	802.1X-REV		
	LinkSec Security Policy:	Not in Use 🛛 👻	
	URL Redirect When a URL is defined for R	edirect an ACL m	ust also be defined
	URL for Redirect:	Not in Use 🛛 👻	
	URL Redirect ACL:	Not in Use 🔹	]

8. Naviguez jusqu'à Access Policies > Access Services > Default Network Access, puis cliquez sur l'onglet Allowed Protocols. Cochez la case Autoriser PEAP.



9. Accédez à Identité et définissez les règles afin d'autoriser les utilisateurs PEAP.

► 🔂 My Workspace	Access Policies > Access Services > Default Network Access > Identity								
Interview Resources	<ul> <li>Single result selection</li></ul>								
Users and Identity Stores	Identity Policy								
Policy Elements	Filter: Status - Match If. Equals - Clear Filter Go -								
<ul> <li>Access Policies</li> </ul>	-		Status	Name	Conditions		Results		
<ul> <li>Access Services</li> <li>Capito Selection Puller</li> </ul>					Eap Authentication Method	Eap Tunnel Building Method	Identity Source	Hit Count	
O Default Device Admin	1	<b>F</b> 1	Θ	Peap	-ANY-	match PEAP	Internal Users	32	
<ul> <li>O Default Network Access</li> </ul>	2		Θ	Leap	match LEAP	-ANY-	Internal Users	0	
dentity Authorization	3		0	Eapfast	-ANY-	match EAP-FAST	Internal Users	3	
Monitoring and Reports									
System Administration									

10. Naviguez jusqu'à **Autorisation**, et associez Étudiant et enseignant à la Politique d'autorisation ; dans cet exemple, le mappage doit être Student pour VLAN 30 et Teacher pour VLAN 40.

+ 😌 MyWorkspace	Norkspace Access Pokies > Access Services > Celaut Network Access > Authorization										
In Network Resources	Stan	dard P	olicy Exce	eption Polic	x						
Series and identity Stores Network Access Authoritation Policy											
Polygements Place Server + Method Server + Color Floor - Color Floor											
Access Policies		101. VI	anary .		· menerre, support						
Access Senices     H Senice Selection Rules			Status	Name	Eap Authentication Method	Eap Tunnel Building Method	Compound Condition	Protocol	klentity Group	Results Authorization Profiles	Hit Count
O Default Device Admin	1	12		Student	-ANY-	match PEAP	-ANY-	match Radius	in All Groups Students	Student	11
<ul> <li>O Default Network Access</li> <li>Meethy</li> </ul>	2			Teacher	-ANY-	match PEAP	-ANY-	match Radius	in Al Groups Teachers	leacher	4
Autorization	3	12	•	EAPTLS	-ANY-	match EAP-FAST	-ANY-	match Radius	-ANY-	Permit Access	3
<ul> <li>Monitoring and Reports</li> </ul>											
Bystem Administration											

# Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Voici les processus de vérification :

• Surveillez la page de l'ACS qui affiche les clients authentifiés.



• Connectez-vous au réseau local sans fil DVA avec le groupe d'étudiants et examinez l'utilitaire de connexion WiFi du client.

💿 Intel® PRO	Set/Wireless WiFi Connection Utility	
File Tools Adv	anced Profiles Help	
		(intel)
	You are connected to DVA.	
	Network Name:DVASpeed:144.0 MbpsSignal Quality:ExcellentIP Address:30.30.30.2	<u>D</u> etails
WiFi Networ	k <u>s</u> (46)	
alle	DVA     Connecter       This network has security enabled	ed 🛛 😒 😫 🔷
alle	<b>SSID not broadcast&gt;</b> This network has security enabled	a 📇 🛈
alle	SSID not broadcast> This network has security enabled	<mark>9</mark> 40
	<ssid broadcast="" not=""></ssid>	<mark>9</mark>
Disco	nect Prop <u>e</u> rties	<u>R</u> efresh
To manage p Profiles buttor	rofiles of previously connected WiFi networks, clic n.	k the <b>Profiles</b>
	iFi On Hardware radio switch: ON	Help?

• Connectez-vous au réseau local sans fil DVA avec le groupe d'enseignants et examinez l'utilitaire de connexion WiFi du client.

🗑 Intel® PRO	Set/Wireless WiF	i Connection	Utility	
File Tools Adv	anced Profiles Hel	P		
				(intel)
(	You are con	nected to	DVA.	
	Network Name: Speed: Signal Quality: IP Address:	DVA 78.0 Mbps Excellent 40.40.40.2		<u>D</u> etails
WiFi Networ	k <u>s</u> (47)			
alle	DVA This network has se	ecurity enabled	Connected	◎ 8 9 <sup>△</sup> ✓ <sup>△</sup> 0 <sup>△</sup>
alle	SSID not broad This network has set	<b>dcast&gt;</b> ecurity enabled		a 🐸 🛈
alle	SSID not broad This network has set	<b>dcast&gt;</b> ecurity enabled		<mark>9</mark>
all	<ssid broad<="" not="" td=""><td>dcast&gt;</td><td></td><td>a 🐸 🛈 🚽</td></ssid>	dcast>		a 🐸 🛈 🚽
Disco	nect Prop	erties		<u>R</u> efresh
To manage p Profiles buttor	rofiles of previously co n.	nnected WiFi ne	tworks, click the	Profiles
w	iFi On 🔻 🔻	Hardware rad ON	io switch: Hel	p? <u>Close</u>

# Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

## Remarques :

Utilisez l'<u>Outil de recherche de commande (clients inscrits seulement) pour obtenir plus</u> d'informations sur les commandes utilisées dans cette section. L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Les débogages utiles incluent **debug client mac-address** *mac*, ainsi que les commandes de trace NGWC suivantes :

- set trace group-wireless-client level debug
- set trace group-wireless-client filter mac xxxx.xxxx.xxxx
- show trace sys-filtrtered-traces

La trace de NGWC n'inclut pas dot1x/AAA. Utilisez donc cette liste complète de traces combinées pour dot1x/AAA :

- set trace group-wireless-client level debug
- set trace wcm-dot1x event level debug
- set trace wcm-dot1x aaa level debug
- set trace aaa wireless events level debug
- set trace access-session core sm level debug
- set trace access-session méthode dot1x level debug
- set trace group-wireless-client filter mac xxxx.xxxx.xxxx
- set trace wcm-dot1x event filter mac xxxx.xxxx.xxxx
- set trace wcm-dot1x aaa filter mac xxxx.xxxx.xxxx
- set trace aaa wireless events filter mac xxxx.xxxx.xxxx
- set trace access-session core sm filter mac xxxx.xxxx.xxxx
- set trace access-session, méthode dot1x filter mac xxxx.xxxx.xxxx
- show trace sys-filtrtered-traces

Lorsque l'affectation de VLAN dynamique fonctionne correctement, vous devriez voir ce type de sortie des débogages :

09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0) Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13) Tunnel-Private-Id (30) [09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30 [09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New GroupIntf: intfChanged: 1 [09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the Reassociation Count 1 for client (of interface VLAN0040) [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761 --More--Clearing Address 40.40.40.2 on mobile [09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override for station 0021.5C8C.C761 [09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: 'VLAN0030', aclName: '' [09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for station ---

[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies to client

[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC) [09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761

[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
 vlanIfName: 'VLAN0030', aclName: ''

--More-- [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761 Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
 vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030' [09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds from WLAN config [09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds [09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XX: Creating a PKC PMKID Cache entry (RSN 1) [09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0

[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (40)
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
--More-- [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761

Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf: VLAN0040 New GroupIntf: intfChanged: 1 [09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for station 0021.5C8C.C761 [09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for station ---[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies to client [09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC) [09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761

[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
 vlanIfName: 'VLAN0040', aclName: ''
 --More-[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy
from source Override Summation:

[09/01/13 12:08:59.553 IST laed 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040' [09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds from WLAN config [09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds [09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID Cache entry (RSN 1)