Configurazione dell'assegnazione dinamica della VLAN con NGWC e ACS 5.2

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Assegnazione dinamica di VLAN con server RADIUS Configurazione Esempio di rete Presupposti Configurazione di WLC con CLI **Configurazione WLAN** Configurazione del server RADIUS su WLC Configurazione del pool DHCP per la VLAN client Configurazione di WLC con GUI **Configurazione WLAN** Configurazione del server RADIUS su WLC **Configura server RADIUS** Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto il concetto di assegnazione dinamica delle VLAN. Viene inoltre descritto come configurare il controller WLC (Wireless LAN Controller) e un server RADIUS in modo da assegnare dinamicamente i client WLAN (Wireless LAN) a una VLAN specifica. In questo documento, il server RADIUS è un Access Control Server (ACS) con Cisco Secure Access Control System versione 5.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Conoscenze base dei WLC e dei Lightweight Access Point (LAP)

- Conoscenza funzionale del server di autenticazione, autorizzazione e accounting (AAA)
- Conoscenza approfondita delle reti wireless e dei problemi di sicurezza wireless

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller LAN wireless Cisco 5760 con software Cisco IOS[®] XE versione 3.2.2 (NGWC, Next Generation Wiring Closet)
- Cisco Aironet serie 3602 Lightweight Access Point
- Microsoft Windows XP con Intel Proset Supplicant
- Cisco Secure Access Control System versione 5.2
- Cisco Catalyst serie 3560 Switch

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Assegnazione dinamica di VLAN con server RADIUS

Nella maggior parte dei sistemi WLAN, ogni WLAN dispone di un criterio statico che viene applicato a tutti i client associati a un SSID (Service Set Identifier) o a una WLAN nella terminologia del controller. Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

Tuttavia, la soluzione Cisco WLAN supporta le reti di identità. Ciò consente alla rete di annunciare un singolo SSID, ma permette a utenti specifici di ereditare diversi attributi QoS e VLAN e/o criteri di sicurezza in base alle credenziali dell'utente.

L'assegnazione dinamica della VLAN è una di queste funzionalità che permette a un utente wireless di accedere a una VLAN specifica in base alle credenziali fornite dall'utente. Questa attività di assegnazione degli utenti a una VLAN specifica viene gestita da un server di autenticazione RADIUS, ad esempio Cisco Secure ACS. Questa funzione può essere utilizzata, ad esempio, per consentire all'host wireless di rimanere sulla stessa VLAN su cui si sposta all'interno della rete di un campus.

Di conseguenza, quando un client tenta di associarsi a un LAP registrato con un controller, il LAP passa le credenziali dell'utente al server RADIUS per la convalida. Una volta completata l'autenticazione, il server RADIUS passa all'utente alcuni attributi IETF (Internet Engineering Task Force). Questi attributi RADIUS determinano l'ID VLAN da assegnare al client wireless. L'SSID del client (la WLAN, nei termini del WLC) non conta perché l'utente è sempre assegnato a questo ID VLAN predeterminato.

Gli attributi utente RADIUS utilizzati per l'assegnazione dell'ID VLAN sono:

- IETF 64 (Tipo di tunnel): impostato su VLAN.
- IETF 65 (Tunnel Medium Type) Impostato su 802.
- IETF 81 (Tunnel-Private-Group-ID): impostato sull'ID VLAN.

L'ID VLAN è 12 bit e assume un valore compreso tra 1 e 4094 inclusi. Poiché Tunnel-Private-Group-ID è di tipo string, come definito nella <u>RFC 2868, RADIUS Attributes for Tunnel Protocol</u> <u>Support</u> for use with IEEE 802.1X, il valore intero dell'ID VLAN viene codificato come stringa. Quando vengono inviati questi attributi del tunnel, è necessario compilare il campo Tag.

Come indicato nella RFC 2868, sezione 3.1:

"Il campo Tag è lungo un ottetto e serve a raggruppare gli attributi dello stesso pacchetto che fanno riferimento allo stesso tunnel."

I valori validi per il campo Tag sono compresi tra 0x01 e 0x1F inclusi. Se il campo Tag non è utilizzato, deve essere zero (0x00). Per ulteriori informazioni su tutti gli attributi RADIUS, consultare la RFC 2868.

Configurazione

La configurazione di un'assegnazione dinamica di VLAN prevede due passaggi distinti:

- 1. Configurare il WLC con l'interfaccia della riga di comando (CLI) o con la GUI.
- 2. Configurare il server RADIUS.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento</u> <u>di ricerca dei comandi (solo utenti registrati).</u>

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nel documento viene usato 802.1X con PEAP (Protected Extensible Authentication Protocol) come meccanismo di sicurezza.

Presupposti

- Gli switch sono configurati per tutte le VLAN di layer 3 (L3).
- Al server DHCP viene assegnato un ambito DHCP.
- Esiste una connettività L3 tra tutti i dispositivi della rete.
- II LAP è già unito al WLC.
- Ogni VLAN ha una maschera /24.
- In ACS 5.2 è installato un certificato autofirmato.

Configurazione di WLC con CLI

Configurazione WLAN

Questo è un esempio di come configurare una WLAN con l'SSID di DVA:

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

Configurazione del server RADIUS su WLC

Questo è un esempio della configurazione del server RADIUS sul 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 Cisco123
```

dot1x system-auth-control

Configurazione del pool DHCP per la VLAN client

Questo è un esempio di configurazione del pool DHCP per la VLAN 30 e la VLAN 40 del 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
```

Configurazione di WLC con GUI

Configurazione WLAN

In questa procedura viene descritto come configurare la WLAN.

1. Selezionare Configuration > Wireless > WLAN > NEW (Configurazione > Wireless > WLAN > scheda NEW (NUOVA).



2. Fare clic sulla scheda **General** (Generale) per verificare che la WLAN sia configurata per WPA2-802.1X e mappare l'interfaccia/il gruppo di interfacce (G) alla VLAN 20 (**VLAN0020**).

WLAN 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) Broadcast SSID Multicast VLAN Feature	VLAN0020 ▼ ✓

 Fare clic sulla scheda Advanced (Avanzate) e selezionare la casella di controllo Allow AAA Override (Consenti sostituzione AAA). Per il corretto funzionamento di questa funzionalità è necessario attivare l'override.

WLAN WLAN > Edit							
General	Security	QOS	Advanced				
Allow AAA Override Coverage Hole Detection							
Session T	imeout (secs) 1	800				

4. Fare clic sulla scheda **Protezione** e sulla scheda **Layer2**, selezionare la casella di controllo WPA2 Encryption **AES** e selezionare **802.1x** dall'elenco a discesa Auth Key Mgmt.

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

Configurazione del server RADIUS su WLC

In questa procedura viene descritto come configurare il server RADIUS sul WLC.

1. Passare alla scheda **Configurazione > Protezione**.

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

2. Per creare i gruppi di server Radius, selezionare **AAA > Gruppi di server > Radius**. Nell'esempio, il gruppo di server Radius è denominato ACS.

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

3. Modificare la voce Server Radius per aggiungere l'indirizzo IP del server e il segreto condiviso. Questo segreto condiviso deve corrispondere al segreto condiviso sul WLC e sul server RADIUS.

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

Questo è un esempio di configurazione completa:

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

Configura server RADIUS

In questa procedura viene descritto come configurare il server RADIUS.

- 1. Sul server RADIUS, selezionare Utenti e archivi identità > Archivi identità interni > Utenti.
- 2. Creare i nomi utente e i gruppi di identità appropriati. In questo esempio, è Studente e tutti i gruppi:Studenti e Insegnante e Tutti i gruppi:Insegnanti.



3. Passare a Elementi criterio > Autorizzazioni e autorizzazioni > Accesso alla rete > Profili di autorizzazione e creare i profili di autorizzazione per la sostituzione AAA.

🕨 😚 My Workspace	Policy Eler	ments > Authorizati	on and Permissions > N	Network Acc	ess > Aut	horization F
Network Resources	Author	rization Profiles				
Users and Identity Stores	Filter:		Match if	-	Go] 🔻	,
🔹 🦻 Policy Elements			Waterrin.			
 Session Conditions 		Name 🔺	Description			
Date and Time		Permit Access				
Custom		Student	Student			
Authorization and Permissions		teacher	teacher			
 Network Access Authorization Profiles Device Administration Named Permission Objects 						
Access Policies						

4. Modificare il profilo di autorizzazione per lo studente.



5. Impostare l'ID/nome della VLAN su Static con un valore di 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. Modificare il profilo di autorizzazione per l'insegnante.

Po	licy ⊟ements > Auth	orization and Pe	ermissions > Network A	ccess > Authorization Profiles > Edit: "teacher"
	General Con	nmon Tasks	RADIUS Attributes	
	🌣 Name:	teacher		
	Description:	teacher		
	Required field	ds		

7. Impostare l'ID/nome della VLAN su Static con un valore di 40 (VLAN 40).

Poli	cy Elements > Authorization and F	Permissions > Netw	ork Access > Authorization Profiles > Edit: "teacher"
	General Common Tasks	RADIUS Attribut	tes
	ACLS	M	
	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 mu	ist also be defined
	URL for Redirect:	Not in Use 🛛 👻	
	URL Redirect ACL:	Not in Use 🔷 👻	

8. Passare a **Criteri di accesso > Servizi di accesso > Accesso di rete predefinito** e fare clic sulla scheda **Protocolli consentiti**. Selezionare la casella di controllo **Consenti PEAP**.



9. Passare a **Identità** e definire le regole per consentire agli utenti PEAP.

► 🔂 My Workspace	Access Policies > Access Services > Default Network Access > Identity									
Interview Resources	0:	 Single result selection								
Users and Identity Stores	Ide	Identity Policy								
Solicy Elements	Filter: Status - Match It: Equals - Clear Filter Go -									
🔹 🛼 Access Policies	-				Con	ditions	Results			
 Access Services Service Selection Pulse 			Status	Name	Eap Authentication Method	Eap Tunnel Building Method	Identity Source	Hit Count		
O Default Device Admin	1	F 1	Θ	Peap	-ANY-	match PEAP	Internal Users	32		
 O Default Network Access 	2		•	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. Passare a **Autorizzazione** e associare Studente e insegnante alla politica di autorizzazione; nell'esempio, la mappatura deve essere Student per la VLAN 30 e Teacher per la VLAN 40.

MyWorkspace	Access Pokies > Access Devices > Default Network Access > Authorization												
Network Resources	Standard Policy Exception Policy												
Stores and identity Stores	N	Network Access Authorization Policy											
PolicyElements Access Policies	R	Filter, Status • Nalch #, Equals • • Clear Filter do •											
Access Senices Senice Selecton Rules O Default Device Admin O Default Network Access Mently Puncerson			Status	Name	Eap Authentication Method	Eap Tunnel Building Method	Compound Condition	Protocol	klentity Group	Results Authorization Profiles	Hit Count		
	1	12		Student	-ANY-	match FEAP	-ANY-	match Radius	in All Groups Students	Student	11		
	2			Teacher	-ANY-	match PEAP	-ANY-	match Radius	In All Groups Teachers	leacher	4		
	3	12		EAPTLS	-ANY-	match EAP-FAST	-ANY-	match Radius	-ANY-	Permit Access	3		
Monitoring and Reports													
Bystem Administration													

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione. Si tratta dei processi di verifica:

• Controllare la pagina su ACS che mostra quali client sono autenticati.

Sep 1,13.456.49.200 AM

 Sep 1,13.456.49.200 AM
 Image: sector: 00-215C-8C-C7-61
 Default Network Access
 PEAP (EAP-MSCHAPA2)
 Default Network Derice: 10.105.135.126
 Capwap1
 acstemplate

 Sep 1,13.450.54.403 AM
 Image: student
 00-215C-8C-C7-61
 Default Network Access
 PEAP (EAP-MSCHAPA2)
 Default Network Derice: 10.105.135.126
 Capwap1
 acstemplate

Connettersi alla rete WLAN DVA con Student Group e verificare l'utilità di connessione WiFi del client.

🗑 Intel® PRO	Set/Wireless WiF	i Connection U	tility	
File Tools Adv	anced Profiles Hel	P		
				(intel)
	You are con	nected to E	OVA.	
	Network Name: Speed: Signal Quality: IP Address:	DVA 144.0 Mbps Excellent 30.30.30.2		<u>D</u> etails
WiFi Networ	rk <u>s</u> (46)			
lle	DVA This network has se	curity enabled	Connected) a g ^ / 📇 🛈
ulla	SSID not broad This network has set		a 🏜 🛈	
. III a	SSID not broad This network has set	dcast> ecurity enabled		<mark>9</mark> 80
	<ssid broa<="" not="" td=""><td>dcast></td><td></td><td>9 40</td></ssid>	dcast>		9 40
Disco	nnect Prop <u>e</u>	erties		Refresh
To manage p Profiles buttor	rofiles of previously co n.	nnected WiFi netw	vorks, click the	Profiles
<u>w</u>	iFi On 📃 🔻	Hardware radio ON	switch: Help?	Close

• Connettersi alla WLAN DVA con il Teacher Group e verificare l'utilità di connessione WiFi del client.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Note:

per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Lo <u>strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show.</u> Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

consultare le <u>informazioni importanti sui comandi di debug prima di usare i comandi di</u> **debug.**

I debug utili includono **debug client mac-address** *mac*, nonché i seguenti comandi di traccia NGWC:

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

La traccia NGWC non include dot1x/AAA, quindi usare questo elenco completo di tracce combinate per dot1x/AAA:

- set trace group-wireless-client level debug
- set trace wcm-dot1x event level debug
- set trace wcm-dot1x aaa level debug
- imposta debug a livello di eventi wireless trace aaa
- imposta debug a livello sm di base della sessione di accesso alla traccia
- set trace access-session method 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 method dot1x filter mac xxxx.xxxx.xxxx
- show trace sys-filtered-traces

Quando l'assegnazione della VLAN dinamica funziona correttamente, dovrebbe essere visualizzato questo tipo di output dei debug:

```
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 1XK: 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 laec 5933] 0021.5C8C.C761 Applying override policy

from source Override Summation:

[09/01/13 12:08:59.553 IST 1aed 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 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)