Configurar a atribuição dinâmica de VLAN com NGWC e ACS 5.2

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius Configurar Diagrama de Rede **Hipóteses** Configurar WLC com CLI **Configurar WLAN** Configurar o servidor RADIUS na WLC Configurar o pool DHCP para a VLAN do cliente Configurar WLC com GUI **Configurar WLAN** Configurar o servidor RADIUS na WLC **Configurar servidor RADIUS** Verificar Troubleshoot

Introduction

Este documento descreve o conceito de atribuição de VLAN dinâmica. Ele também descreve como configurar o controlador de LAN sem fio (WLC) e um servidor RADIUS para atribuir dinamicamente clientes de LAN sem fio (WLAN) a uma VLAN específica. Neste documento, o servidor RADIUS é um Access Control Server (ACS) que executa o Cisco Secure Access Control System versão 5.2.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

• Conhecimento básico do WLC e dos LAPs (Lightweight Access Points, pontos de acesso

leves)

- Conhecimento funcional do servidor de autenticação, autorização e contabilização (AAA)
- Conhecimento completo da rede Wireless e problemas de segurança Wireless

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador de LAN sem fio Cisco 5760 com Cisco IOS[®] XE Software Release 3.2.2 (Next Generation Wiring Closet, ou NGWC)
- Access point Cisco Aironet 3602 Series Lightweight
- Microsoft Windows XP com Intel Proset Supplicant
- Cisco Secure Access Control System versão 5.2
- Switch Cisco Catalyst 3560 Series

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.

Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius

Na maioria de sistemas de WLAN, cada WLAN tem uma política estática que se aplica a todos os clientes associados com um Service Set Identifier (SSID), ou o WLAN na terminologia do controlador. Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

Mas a solução de Cisco WLAN suporta identidades na rede. Isso permite que a rede anuncie um único SSID, mas permite que usuários específicos herdem diferentes QoS, atributos de VLAN e/ou políticas de segurança com base nas credenciais do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. Essa tarefa de atribuição de usuário a uma VLAN específica é tratada por um servidor de autenticação RADIUS, como um Cisco Secure ACS. Esse recurso pode ser usado, por exemplo, para permitir que o host sem fio permaneça na mesma VLAN à medida que se move dentro de uma rede de campus.

Como resultado, quando um cliente tenta se associar a um LAP registrado em um controlador, o LAP passa as credenciais do usuário ao servidor RADIUS para validação. Quando a autenticação é bem sucedida, o servidor Radius passa determinados atributos da Internet Engineering Task Force (IETF) ao usuário. Estes atributos RADIUS decidem a ID da VLAN que deve ser atribuído ao cliente wireless. O SSID do cliente (a WLAN, em termos de WLC) não importa porque o usuário é sempre atribuído a esse ID de VLAN predeterminado.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (Tipo de túnel) Definido como VLAN.
- IETF 65 (Tunnel Medium Type) Definido como 802.
- IETF 81 (Tunnel-Private-Group-ID) Definido como ID da VLAN.

O ID da VLAN é de 12 bits e tem um valor entre 1 e 4094, inclusive. Como Tunnel-Private-Group-ID é do tipo string, como definido em <u>RFC 2868, RADIUS Attributes for Tunnel Protocol Support</u> para uso com IEEE 802.1X, o valor inteiro da ID da VLAN é codificado como uma string. Quando estes atributos de túnel são enviados, é necessário preencher o campo Tag.

Como é explicado na RFC2868, seção 3.1:

"O campo Tag tem um octeto de comprimento e se destina a fornecer um meio de agrupar atributos no mesmo pacote que se referem ao mesmo túnel."

Os valores válidos para o campo Tag são 0x01 a 0x1F, inclusive. Se o campo Tag não for utilizado, ele deve ser zero (0x00). Consulte na RFC 2868 mais informações sobre todos os atributos de RADIUS.

Configurar

A configuração de uma atribuição de VLAN dinâmica consiste em duas etapas distintas:

- 1. Configure o WLC com a interface de linha de comando (CLI) ou com a GUI.
- 2. Configure o servidor RADIUS.

Note: Use a <u>Command Lookup Tool (somente clientes registrados) para obter mais</u> informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este documento usa 802.1X com PEAP (Protected Extensible Authentication Protocol) como mecanismo de segurança.

Hipóteses

- Os switches são configurados para todas as VLANs de Camada 3 (L3).
- O servidor DHCP recebe um escopo DHCP.
- A conectividade L3 existe entre todos os dispositivos na rede.
- O LAP já está associado à WLC.
- Cada VLAN tem uma máscara /24.
- O ACS 5.2 tem um certificado autoassinado instalado.

Configurar WLC com CLI

Este é um exemplo de como configurar uma WLAN com o SSID do DVA:

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

Configurar o servidor RADIUS na WLC

Este é um exemplo da configuração do servidor RADIUS na 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

Configurar o pool DHCP para a VLAN do cliente

Este é um exemplo da configuração do pool DHCP para a VLAN 30 e VLAN 40 do cliente:

```
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
```

Configurar WLC com GUI

Configurar WLAN

Este procedimento descreve como configurar a WLAN.

1. Navegue até a guia Configuration > Wireless > WLAN > NEW.

	diadia cisco w	/ireless Con	troller		
:	🏠 Home	Monitor 🛛 🔻	Configuration 💌	Ac	ministration
Wireless		Wizard	LANs		
• V	VLAN		Controller	M	obility Anchor
	UWLANs		Wireless Security		Profile
► A	ccess Points		Commands		
▶ 8	02.11a/n				wpa2psk
▶ 8	02.11h/a/n				noonradius

2. Clique na guia **Geral** para ver se a WLAN está configurada para WPA2-802.1X e mapeie a Interface/Grupo de Interface(G) para a 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)	VLAN0020 -				
Broadcast SSID					
Multicast VLAN Feature					

3. Clique na guia **Avançado** e marque a caixa de seleção **Permitir substituição de AAA**. A substituição deve estar habilitada para que este recurso funcione.

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

4. Clique na guia **Security** e na guia **Layer2**, marque a caixa de seleção WPA2 Encryption **AES** e selecione **802.1x** na lista suspensa Auth Key Management.

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 -							

Configurar o servidor RADIUS na WLC

Este procedimento descreve como configurar o servidor RADIUS na WLC.

1. Navegue até a guia Configuração > Segurança.



2. Navegue até **AAA** > **Server Groups** > **Radius** para criar os Radius Server Groups. Neste exemplo, o Grupo de Servidores Radius é chamado de ACS.

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

3. Edite a entrada do Servidor Radius para adicionar o Endereço IP do Servidor e o Segredo Compartilhado. Esse segredo compartilhado deve corresponder ao segredo compartilhado no WLC e no servidor 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		

Este é um exemplo de uma configuração completa:

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

Configurar servidor RADIUS

Este procedimento descreve como configurar o servidor RADIUS.

- 1. No servidor RADIUS, navegue para Usuários e armazenamento de identidade > Repositórios internos de identidade > Usuários.
- 2. Crie os nomes de usuário e grupos de identidade apropriados. Neste exemplo, é aluno e todos os grupos:alunos, professor e todos os grupos:professores.



3. Navegue até Elementos de política > Autorização e permissões > Acesso à rede > Perfis de autorização e crie os Perfis de autorização para substituição de AAA.

🕨 😚 My Workspace	Policy Bements > Authorization and Permissions > Network Access > Authorization					
Network Resources	Author	Authorization Profiles				
Users and Identity Stores	Filter		Match if	-	Go 🔻	
🔹 🧇 Policy Elements			Materi II.			
 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. Edite o perfil de autorização do aluno.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"								
General Co	General Common Tasks RADIUS Attributes							
Name:	Student							
Description	n: Student							
Required fields								

5. Defina o ID/nome da VLAN como estático com um valor de 30 (VLAN 30).

Pol	cy Elements > Authorization and F	Permissions > Netwo	ork Access > Authorization Profiles > Edit: "Student"
Γ	General Common Tasks	RADIUS Attribut	es
	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		
L	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 mu	stalso be defined
	URL for Redirect:	Not in Use 🗸 👻	
	URL Redirect ACL:	Not in Use 🔹 👻	
	= Required fields		

6. Edite o perfil de autorização do professor.

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. Defina o ID/nome da VLAN como estático com um valor de 40 (VLAN 40).

Poli	cy Elements > Authorization and F	Permissions > Netw	ork Access > Authorization Profiles > Edit: "teacher"
	General Common Tasks	RADIUS Attribu	tes
	ACL\$	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 m	ust also be defined
	URL for Redirect:	Not in Use 🛛 👻	
	URL Redirect ACL:	Not in Use 🔹]

8. Navegue até Access Policies > Access Services > Default Network Access e clique na guia Allowed Protocols. Marque a caixa de seleção Permitir PEAP.



9. Navegue até Identidade e defina as regras para permitir usuários PEAP.

► 🔂 My Workspace	Access Policies > Access Services > Default Network Access > Identity							
Interview Resources	Single result selection Rule based result selection							
Users and Identity Stores	Identity Policy							
Policy Elements	Filter: Status - Match If. Equals - Clear Filter Go -							
🔹 🛼 Access Policies					Con	ditions	Recults	
 Access Services Convice Selection Pulse 			Status	Name	Eap Authentication Method	Eap Tunnel Building Method	Identity Source	Hit Count
O Default Device Admin	1	<u>F1</u>	0	Peap	-ANY-	match PEAP	Internal Users	32
* O Default Network Access	2		0	Leap	match LEAP	-ANY-	Internal Users	0
Authorization	3		Θ	Eapfast	-ANY-	match EAP-FAST	Internal Users	3
Monitoring and Reports								
System Administration								

10. Navegue até **Autorização** e mapeie o aluno e o professor para a Política de Autorização; neste exemplo, o mapeamento deve ser Student para VLAN 30 e Teacher para VLAN 40.

MyWorkspace	My Workspace Access Policies > Access Sorvices > Default Network Access > Authorization										
B Network Resources	Standard Policy Exception Policy										
Users and Identity Stores	N	Notwork Access Authorization Policy									
PolicyElements Access Policies	nents Filter: Status Match If: Equals										
Access Senices Honice Selection Rules			Status	Name	Eap Authentication Method	C Eap Tunnel Building Method	Compound Condition	Protocol	klenilly Group	Results Authorization Profiles	Hit Count
 O Default Device Admin 	1	12		Student	-ANY-	match FEAP	-ANY-	match Radius	in All Groups Students	Student	11
 O Default Network Access Meethy 	2		•	Teacher	-ANY-	match PEAP	-ANY-	match Radius	In All Groups Teachers	teacher	4
Autorization	3	12		EAPTLS	-ANY-	match EAP-FAST	-ANY-	match Radius	-ANY-	Permit Access	3
Monitoring and Reports											
» 🥞 Bystem Administration											

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Estes são os processos de verificação:

• Monitore a página no ACS que mostra quais clientes estão autenticados.



 Conecte-se à WLAN DVA com o grupo de alunos e examine o Utilitário de Conexão WiFi do cliente.

🗑 Intel® PRO	Set/Wireless WiF	i Connection (Jtility	
File Tools Adv	anced Profiles Hel	p		
				(intel)
	You are con	nected to I	DVA.	
	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)			
ulle	DVA This network has se	curity enabled	Connected	● a 9 ^ ⁄ ≛ 0
lle	SSID not broad This network has set	dcast> ecurity enabled		a 🐸 🛈
Ile	SSID not broad This network has set	dcast> curity enabled		<mark>9</mark> 40
II	<ssid broad<="" not="" td=""><td>dcast></td><td></td><td><mark>9</mark></td></ssid>	dcast>		<mark>9</mark>
Disco	nnect Prop <u>e</u>	erties		<u>R</u> efresh
To manage p Profiles buttor	rofiles of previously co n.	nnected WiFi net	works, click the	Profiles
<u>w</u>	iFi On 🔍 🔻	Hardware radio ON	o switch: Help?	Close

 Conecte-se à WLAN DVA com o grupo de professores e consulte o Utilitário de Conexão WiFi do cliente.

🗑 Intel® PRO	Set/Wireless WiF	i Connection	Utility	
File Tools Adv	vanced Profiles He	lp		
				intel
	You are con	inected to	DVA.	
	Network Name: Speed: Signal Quality: IP Address:	DVA 78.0 Mbps Excellent 40.40.40.2		Details
- WiFi Netwo	ork <u>s</u> (47)			
alla	DVA This network has se	ecurity enabled	Connected	
. III d	SSID not broa This network has set	dcast> ecurity enabled		a 🐸 🛈
. III d	SSID not broa This network has set	dcast> ecurity enabled		<mark>9</mark>
all	<ssid broa<="" not="" td=""><td>dcast></td><td></td><td>a 🐸 🛈 🗸</td></ssid>	dcast>		a 🐸 🛈 🗸
Disco	nect Prop	erties		<u>R</u> efresh
To manage p Profiles butto	profiles of previously co n.	onnected WiFi ne	tworks, click the	Profiles
<u> </u>	<u>V</u> iFi On	Hardware radi ON	io switch: Help?	Close

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Notas:

Use a <u>Command Lookup Tool (somente clientes registrados)</u> para obter mais informações sobre os comandos usados nesta seção.

A <u>ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com</u> <u>alguns comandos de exibição.</u>. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Consulte <u>Informações Importantes sobre Comandos de Depuração antes de usar comandos</u> **debug.**

As depurações úteis incluem **debug client mac-address** *mac*, bem como estes comandos de rastreamento NGWC:

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

O rastreamento NGWC não inclui dot1x/AAA, portanto, use esta lista inteira de rastreamentos combinados para 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 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-filtrated-traces

Quando a atribuição de VLAN dinâmica está funcionando corretamente, você deve ver esse tipo de saída das depurações:

```
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 1aec 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)