

Configuración de la Asignación de VLAN Dinámica con NGWC y ACS 5.2

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Asignación de VLAN Dinámica con Servidor RADIUS](#)

[Configurar](#)

[Diagrama de la red](#)

[Suposición](#)

[Configuración de WLC con CLI](#)

[Configuración de WLAN](#)

[Configuración del servidor RADIUS en WLC](#)

[Configuración del Conjunto DHCP para la VLAN del Cliente](#)

[Configuración de WLC con GUI](#)

[Configuración de WLAN](#)

[Configuración del servidor RADIUS en WLC](#)

[Configurar servidor RADIUS](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el concepto de asignación de VLAN dinámica. También describe cómo configurar el controlador de LAN inalámbrica (WLC) y un servidor RADIUS para asignar clientes de LAN inalámbrica (WLAN) a una VLAN específica dinámicamente. En este documento, el servidor RADIUS es un servidor de control de acceso (ACS) que ejecuta Cisco Secure Access Control System versión 5.2.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del WLC y los puntos de acceso ligeros (LAP)

- Conocimiento funcional del servidor de autenticación, autorización y contabilidad (AAA)
- Conocimiento completo de las redes inalámbricas y de los problemas de seguridad inalámbrica

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador de LAN inalámbrica Cisco 5760 con Cisco IOS® XE Software versión 3.2.2 (armario de cableado de última generación o NGWC)
- Cisco Aironet 3602 Series Lightweight Access Point
- Microsoft Windows XP con suplicante Intel Proset
- Cisco Secure Access Control System versión 5.2
- Switch Cisco Catalyst serie 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.

Asignación de VLAN Dinámica con Servidor RADIUS

En la mayoría de los sistemas WLAN, cada WLAN tiene una política estática que se aplica a todos los clientes asociados a un identificador de conjunto de servicios (SSID) o WLAN en la terminología del controlador. Aunque poderoso, este método tiene limitaciones porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes QoS y políticas de seguridad.

Sin embargo, la solución de WLAN de Cisco admite redes de identidad. Esto permite que la red anuncie un SSID único y que usuarios específicos hereden diferentes políticas de QoS, atributos de VLAN o políticas de seguridad en función de las credenciales del usuario.

La asignación de VLAN dinámica es una de estas funciones que colocan a un usuario inalámbrico en una VLAN específica en función de las credenciales suministradas por el usuario. Esta tarea de asignación de usuario a una VLAN específica es manejada por un servidor de autenticación RADIUS, como un Cisco Secure ACS. Esta función se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en la misma VLAN a medida que se desplaza dentro de una red de campus.

Como resultado, cuando un cliente intenta asociarse a un LAP registrado con un controlador, el LAP pasa las credenciales del usuario al servidor RADIUS para la validación. Cuando la autenticación es correcta, el servidor RADIUS transmite una serie de atributos del Grupo de trabajo en ingeniería de Internet (IETF) al usuario. Estos atributos de RADIUS deciden la ID de VLAN que se debe asignar al cliente inalámbrico. El SSID del cliente (la WLAN, en términos del WLC) no importa porque el usuario siempre está asignado a este ID de VLAN predeterminado.

Los atributos del usuario de RADIUS que se utilizan para la asignación del ID de VLAN son:

- IETF 64 (Tipo de túnel): Defina en VLAN.
- IETF 65 (tipo de túnel medio): Defina en 802.

- IETF 81 (Tunnel-Private-Group-ID): Defina el ID de VLAN.

El ID de VLAN es de 12 bits y toma un valor entre 1 y 4094, ambos inclusive. Debido a que el Tunnel-Private-Group-ID es de tipo string, como se define en [RFC 2868, RADIUS Attributes for Tunnel Protocol Support](#) para su uso con IEEE 802.1X, el valor entero de ID de VLAN se codifica como una cadena. Una vez que se envían estos atributos del túnel, es necesario rellenar el campo Tag (Etiqueta).

Como se indica en RFC2868 , sección 3.1:

"El campo Tag tiene un octeto de longitud y su objetivo es proporcionar un medio para agrupar atributos en el mismo paquete que se refieran al mismo túnel."

Los valores válidos para el campo Tag son 0x01 a 0x1F, ambos inclusive. Si el campo Tag (Etiqueta) no se utiliza, debe tener el valor cero (0x00). Consulte RFC 2868 para obtener más información sobre todos los atributos de RADIUS.

Configurar

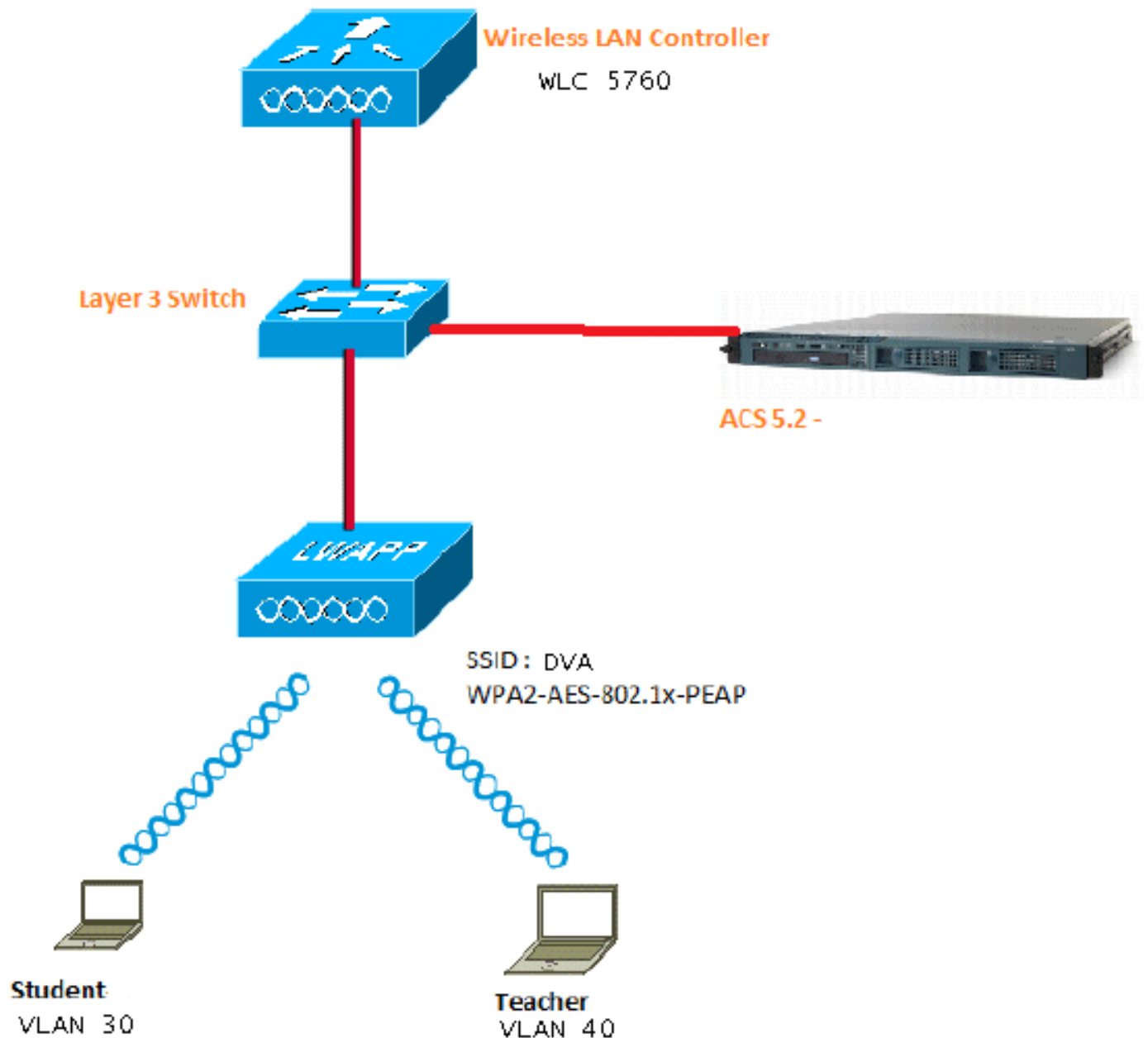
La configuración de una asignación de VLAN dinámica consta de dos pasos distintos:

1. Configure el WLC con la interfaz de línea de comandos (CLI) o con la GUI.
2. Configure el servidor RADIUS.

Nota: Use la [Command Lookup Tool \(clientes registrados solamente\) para obtener más información sobre los comandos usados en esta sección.](#)

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este documento utiliza 802.1X con protocolo de autenticación extensible protegido (PEAP) como mecanismo de seguridad.

Suposición

- Los switches se configuran para todas las VLAN de capa 3 (L3).
- Al servidor DHCP se le asigna un alcance DHCP.
- Existe conectividad L3 entre todos los dispositivos de la red.
- El LAP ya está unido al WLC.
- Cada VLAN tiene una máscara /24.
- ACS 5.2 tiene instalado un certificado autofirmado.

Configuración de WLC con CLI

Configuración de WLAN

Este es un ejemplo de cómo configurar una WLAN con el SSID de DVA:

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

Configuración del servidor RADIUS en WLC

Este es un ejemplo de la configuración del servidor RADIUS en el 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
```

Configuración del Conjunto DHCP para la VLAN del Cliente

Este es un ejemplo de la configuración del conjunto DHCP para la VLAN 30 y la VLAN 40 del 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

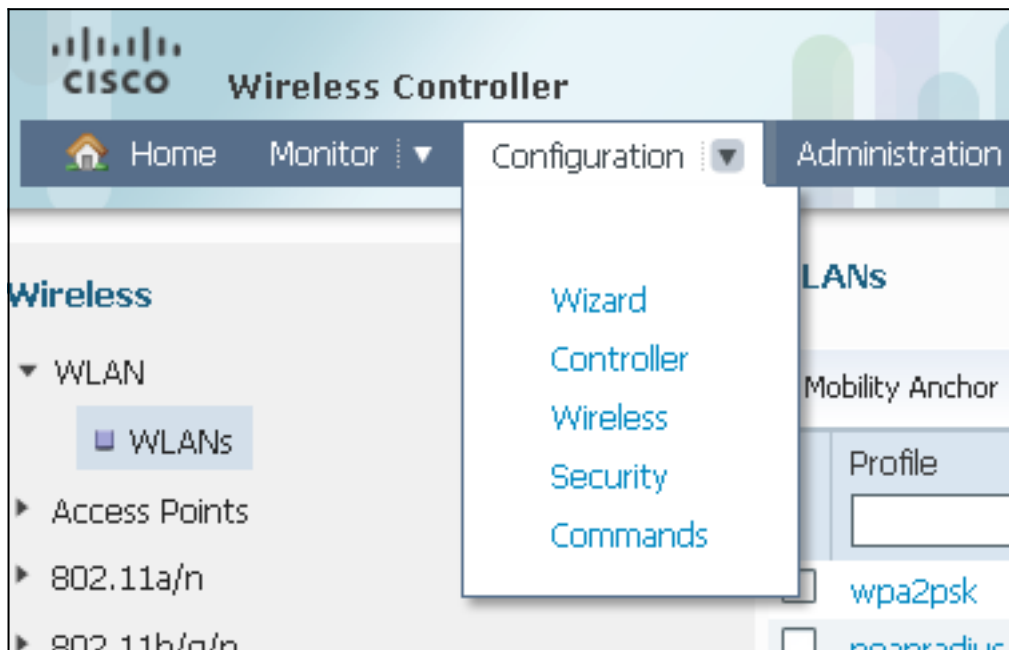
ip dhcp snooping vlan 30,40
ip dhcp snooping
```

Configuración de WLC con GUI

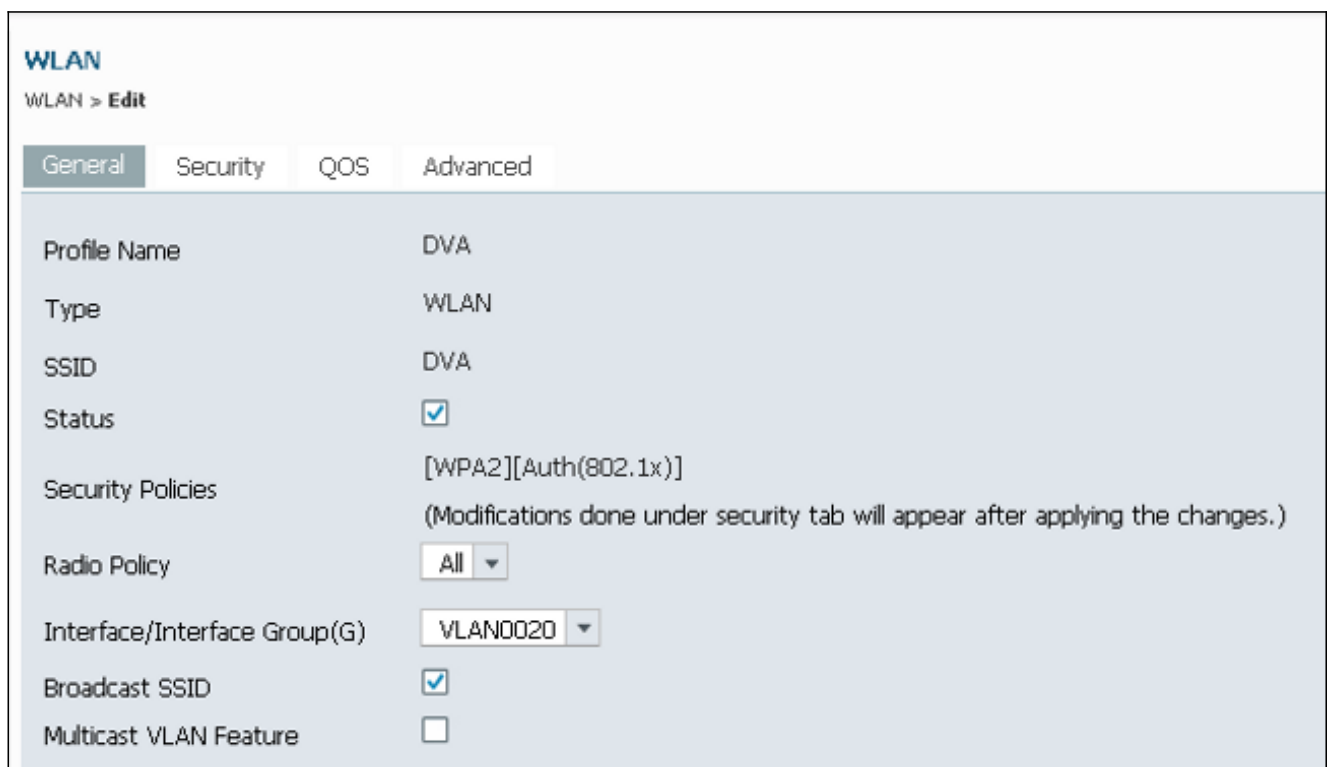
Configuración de WLAN

Este procedimiento describe cómo configurar la WLAN.

1. Vaya a **Configuration > Wireless > WLAN > NEW**.



2. Haga clic en la pestaña **General** para ver que la WLAN está configurada para WPA2-802.1X, y mapee el Grupo de Interfaz/Interfaz (G) a VLAN 20 (**VLAN0020**).



3. Haga clic en la pestaña **Avanzado** y marque la **casilla de verificación Permitir Anulación AAA**. Para que esta función funcione, se debe habilitar la sustitución.

WLAN
WLAN > **Edit**

General Security QOS **Advanced**

Allow AAA Override

Coverage Hole Detection

Session Timeout (secs)

4. Haga clic en la pestaña **Seguridad** y en la pestaña **Capa 2**, active la casilla de verificación **AES** de cifrado WPA2 y seleccione **802.1x** en la lista desplegable Administración de claves de autenticación.

WLAN
WLAN > **Edit**

General **Security** QOS Advanced

Layer2 **Layer3** AAA Server

Layer 2 Security

MAC Filtering

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption AES TKIP

Auth Key Mgmt

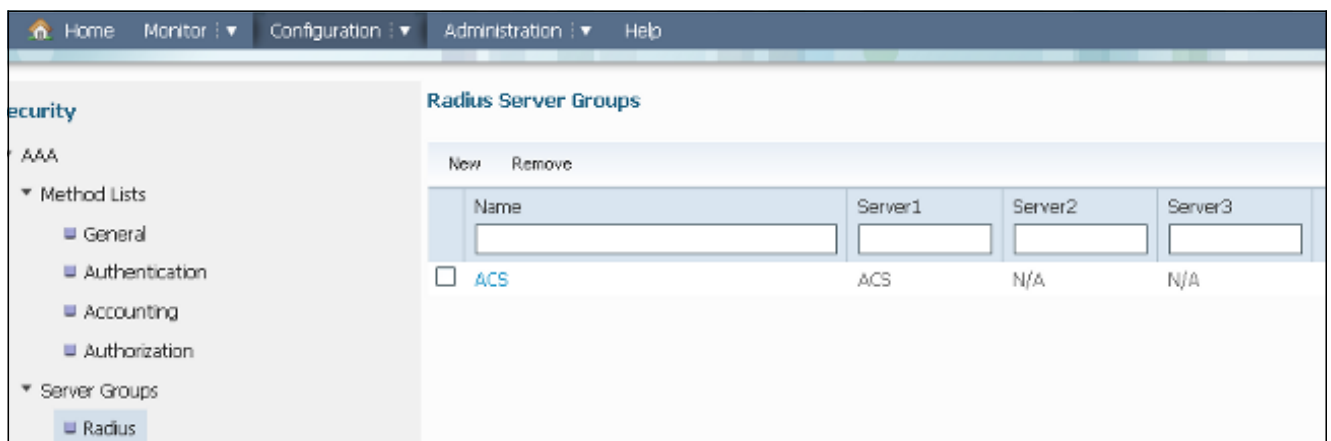
Configuración del servidor RADIUS en WLC

Este procedimiento describe cómo configurar el servidor RADIUS en el WLC.

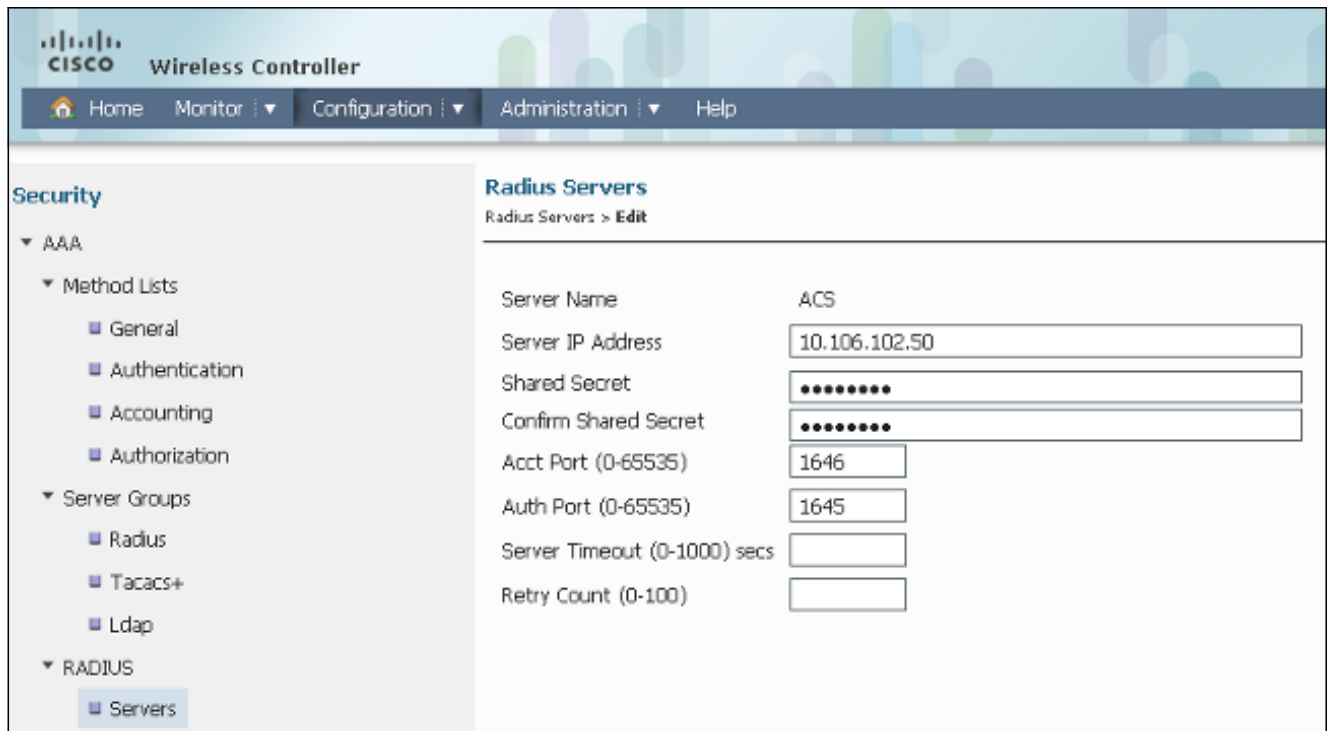
1. Vaya a **Configuration > Security** tab.



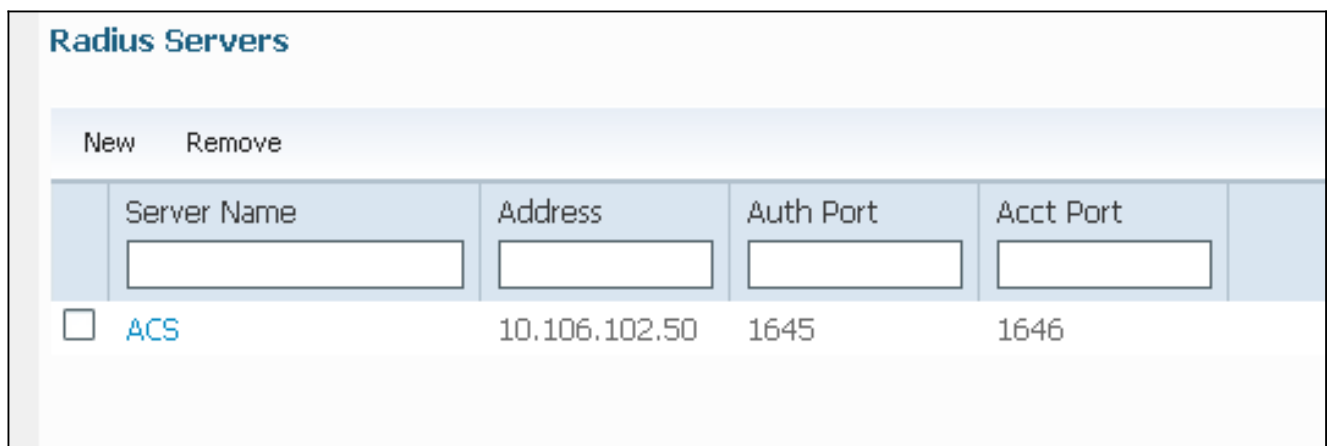
2. Navegue hasta **AAA > Grupos de Servidores > Radius** para crear los Grupos de Servidores Radius. En este ejemplo, el Grupo de servidores Radius se denomina ACS.



3. Edite la entrada del servidor Radius para agregar la dirección IP del servidor y el secreto compartido. Este Secreto Compartido debe coincidir con el Secreto Compartido en el WLC y el servidor RADIUS.



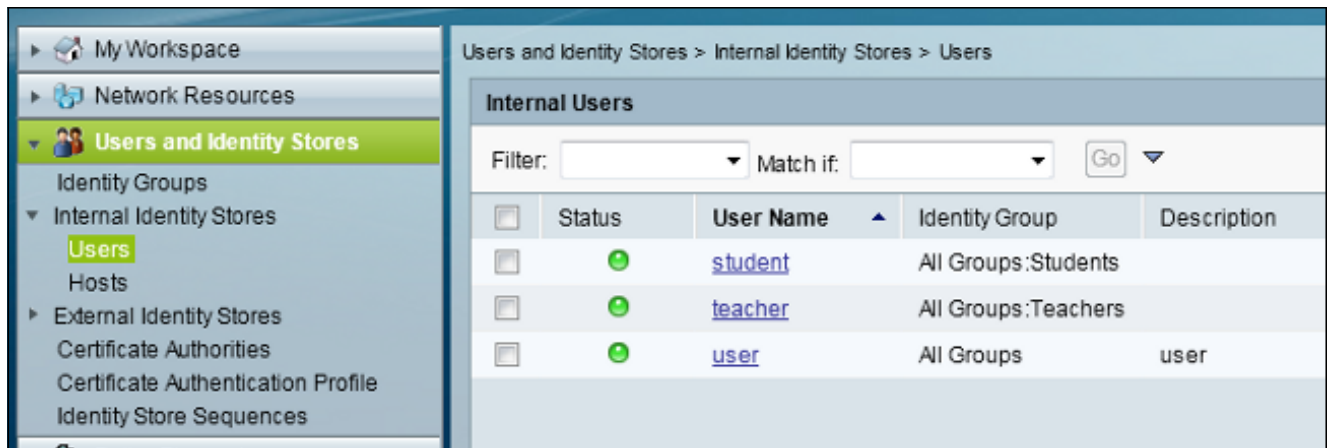
Este es un ejemplo de una configuración completa:



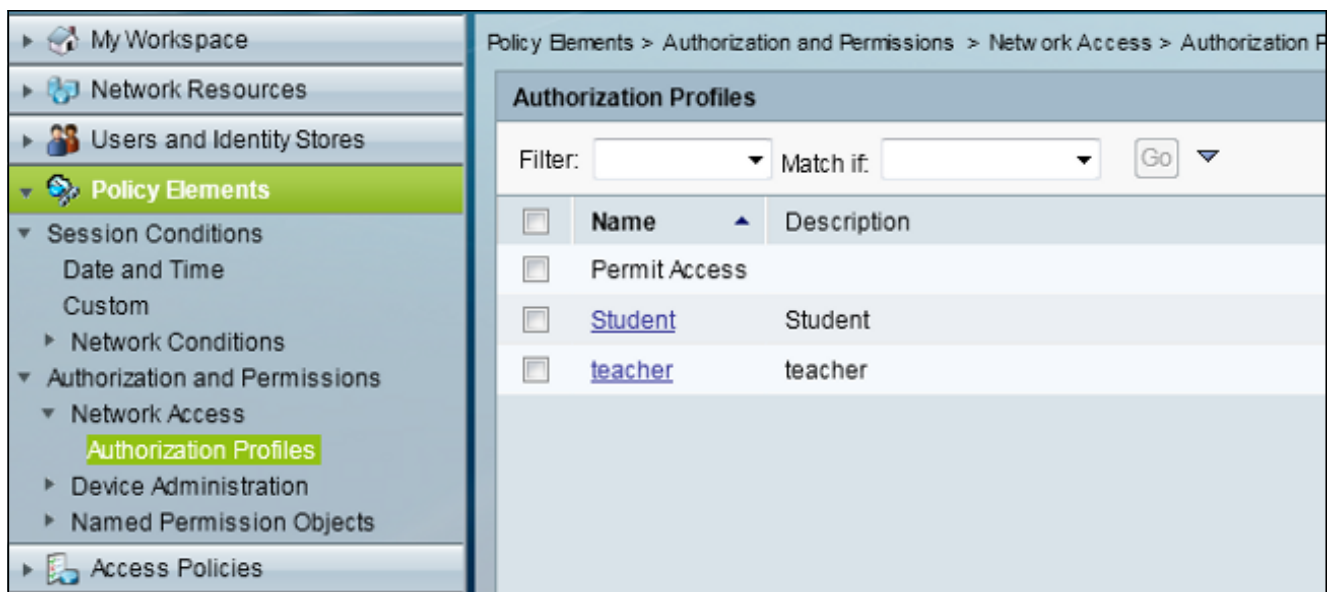
Configurar servidor RADIUS

Este procedimiento describe cómo configurar el servidor RADIUS.

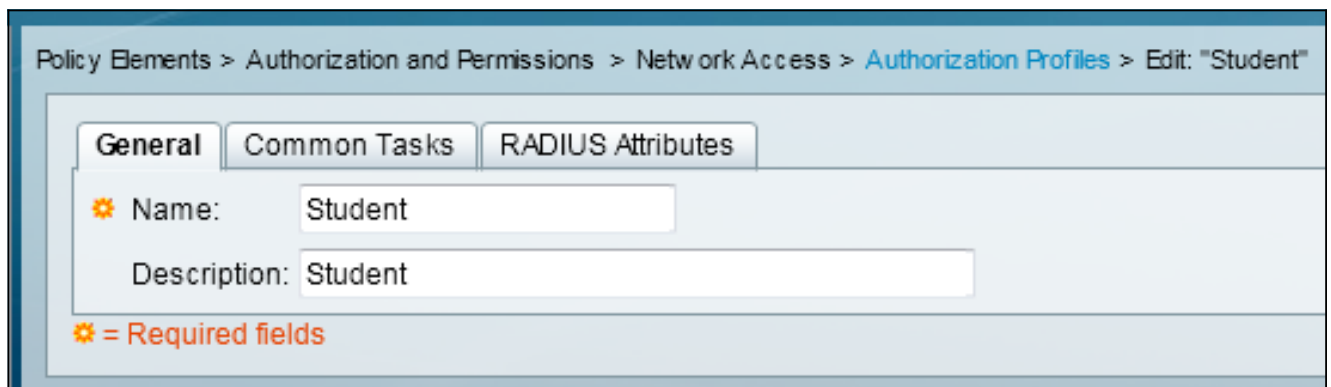
1. En el servidor RADIUS, navegue hasta **Usuarios y Almacenes de Identidad > Almacenes de Identidad Interna > Usuarios**.
2. Cree los nombres de usuario y los grupos de identidad adecuados. En este ejemplo, se trata de Estudiantes y Todos los Grupos:Estudiantes y Profesores y Todos los Grupos:Profesores.



3. Navegue hasta **Elementos de Política > Autorización y Permisos > Acceso a Red > Perfiles de Autorización**, y cree los Perfiles de Autorización para Anulación AAA.



4. Editar el perfil de autorización para el alumno.



5. Configure el ID/Nombre de VLAN como **Estático** con un Valor de **30** (VLAN 30).

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"

General Common Tasks RADIUS Attributes

ACLS
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 30

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 Redirect an ACL must also be defined
URL for Redirect: Not in Use
URL Redirect ACL: Not in Use

⚙ = Required fields

6. Edite el perfil de autorización del profesor.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "teacher"

General Common Tasks RADIUS Attributes

⚙ Name: teacher
Description: teacher

⚙ = Required fields

7. Configure el ID/Nombre de VLAN como **Estático** con un Valor de **40** (VLAN 40).

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "teacher"

General Common Tasks RADIUS Attributes

ACLS

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 ▼

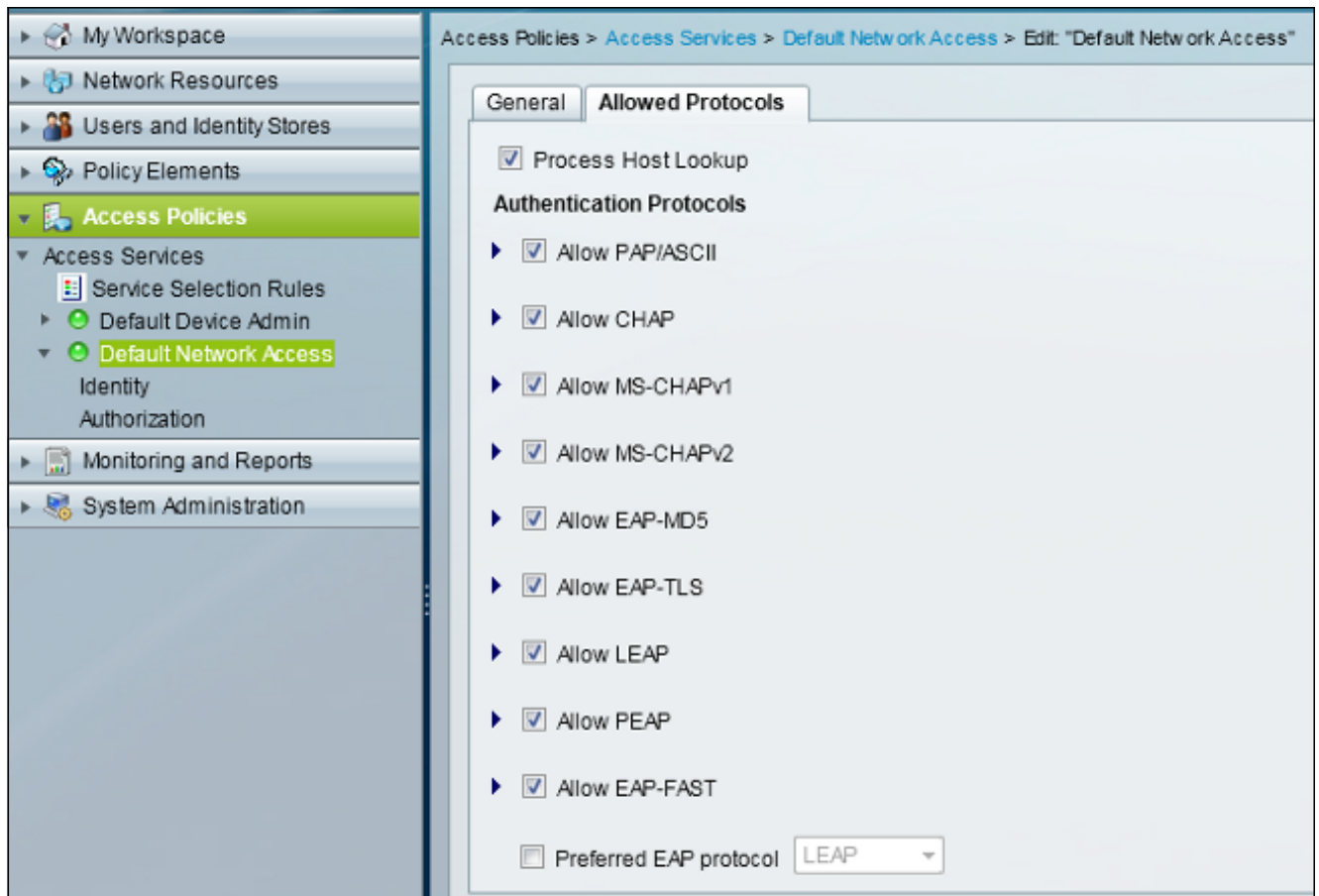
URL Redirect

When a URL is defined for Redirect an ACL must also be defined

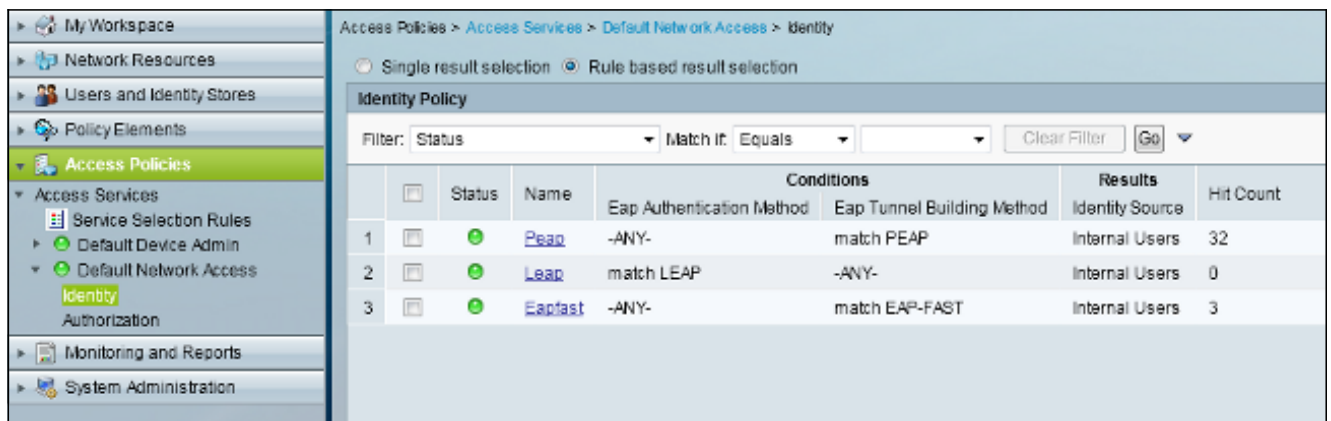
URL for Redirect: Not in Use ▼

URL Redirect ACL: Not in Use ▼

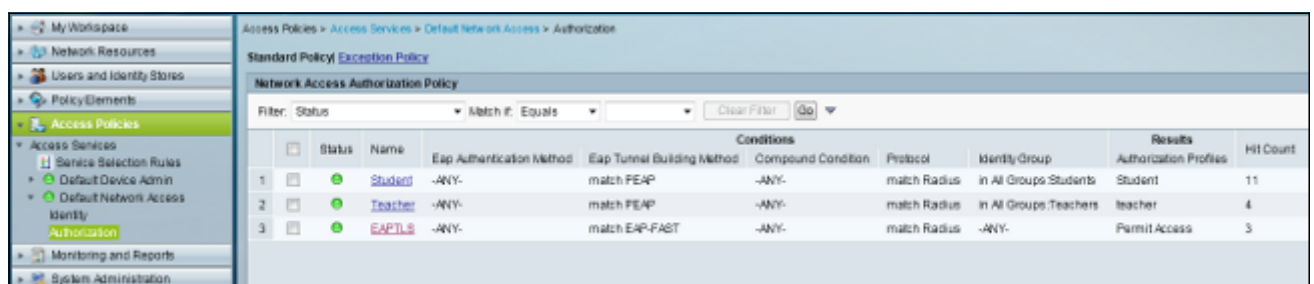
8. Navegue hasta **Políticas de acceso > Servicios de acceso > Acceso de red predeterminado**, y haga clic en la pestaña **Protocolos permitidos**. Marque la casilla **Allow PEAP** .



9. Navegue hasta **Identidad**, y defina las reglas para permitir usuarios PEAP.



10. Navegue hasta **Autorización**, y mapee Estudiantes y Profesores a la Política de Autorización; en este ejemplo, el mapping debe ser Student for VLAN 30 y Teacher for VLAN 40.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente. Estos son los procesos de verificación:


- Supervise la página en el ACS que muestra qué clientes están autenticados.


Sep 1, 13:45:49.220 AM	✓	teacher	00-21-5C-8C-C7-81	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Device	10.105.135.176	Capwap1	acstemplate
Sep 1, 13:45:54.483 AM	✓	student	00-21-5C-8C-C7-81	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Device	10.105.135.176	Capwap1	acstemplate

- Conéctese a la WLAN DVA con el grupo de alumnos y revise la utilidad de conexión WiFi del cliente.

Intel® PROSet/Wireless WiFi Connection Utility

File Tools Advanced Profiles Help










 **You are connected to DVA.**

Network Name: DVA
Speed: 144.0 Mbps
Signal Quality: Excellent
IP Address: 30.30.30.2

[Details...](#)

WiFi Networks (46)

	DVA Connected	
	<SSID not broadcast>	
	<SSID not broadcast>	
	<SSID not broadcast>	

[Disconnect](#) [Properties...](#) [Refresh](#)

To manage profiles of previously connected WiFi networks, click the Profiles button. [Profiles...](#)

[WiFi On](#) Hardware radio switch: ON [Help?](#) [Close](#)

- Conéctese a la WLAN de DVA con el Teacher Group y revise la utilidad de conexión WiFi del cliente.

The screenshot shows the Intel PROSet/Wireless WiFi Connection Utility window. The title bar reads "Intel® PROSet/Wireless WiFi Connection Utility" with standard window controls. The menu bar includes "File", "Tools", "Advanced", "Profiles", and "Help". The main content area features the Intel logo in the top right and a large heading "You are connected to DVA." accompanied by a wireless signal icon. Below this, connection statistics are listed: Network Name: DVA, Speed: 78.0 Mbps, Signal Quality: Excellent, and IP Address: 40.40.40.2. A "Details..." button is positioned to the right of these statistics. A section titled "WiFi Networks (47)" contains a list of networks. The first entry, "DVA", is highlighted and marked as "Connected". It shows a signal strength bar, a lock icon, and the text "This network has security enabled". To its right are icons for wireless standards (a, g, n) and a checkmark. Below this are three entries with "<SSID not broadcast>" and two entries with "<SSID not broadcast>" and a signal strength bar. At the bottom of the network list are "Disconnect", "Properties...", and "Refresh" buttons. Below the network list, a text box states: "To manage profiles of previously connected WiFi networks, click the Profiles button." with a "Profiles..." button to its right. At the very bottom, there is a "WiFi On" button with a dropdown arrow, the text "Hardware radio switch: ON", a "Help?" link, and a "Close" button.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Notas:

Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando show.

Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Los debugs útiles incluyen **debug client mac-address mac**, así como estos comandos de seguimiento de NGWC:

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

El seguimiento de NGWC no incluye dot1x/AAA, así que utilice toda esta lista de seguimientos 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-filtered-traces**

Cuando la asignación de VLAN dinámica funciona correctamente, debería ver este tipo de salida de las depuraciones:

```
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)
--More-- [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
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)