UNIVERSIDAD DEL NORTE

DIRECCION EN TECNOLOGIA INFORMATICA Y DE COMUNICACIONES

GUIA DE INSTALACIÓN Y CONFIGURACIÓN
WIRELESS LAN CONTROLLER (WLC)

Barranquilla, diciembre 2021

Contenido

1 Introducción

En este artículo, veremos una configuración básica paso a paso de un controlador de LAN inalámbrica de Cisco. Antes de seguir adelante, veamos primero algunos conceptos básicos sobre el producto y la tecnología wlan de Cisco:

Cisco introdujo dos tipos de arquitecturas inalámbricas en su cartera de WiFi:

- Arquitectura distribuida.
- Arquitectura centralizada.

Arquitectura WiFi distribuida: en la arquitectura distribuida, todos los puntos de acceso WiFi (AP) son autónomos y se llaman AP autónomos o independientes. Los AP autónomos funcionan individualmente y deben configurarse y administrarse uno por uno. En esta arquitectura, un punto de acceso autónomo realiza operaciones de operación y administración de 802.11.

Arquitectura WiFi centralizada: en la Arquitectura centralizada, los puntos de acceso son controlados y administrados por un dispositivo central llamado Controlador de LAN inalámbrica (WLC) y dichos puntos de acceso se llaman AP de peso ligero. Un punto de acceso ligero realiza solo la operación 802.11 en tiempo real. Todas las funciones de administración se realizan generalmente en un controlador de LAN inalámbrica. Un AP ligero no puede funcionar por sí solo.

Antes de saltar a la configuración, hablemos un poco sobre los puertos del controlador de LAN inalámbrica, las interfaces del controlador y el protocolo CAPWAP.

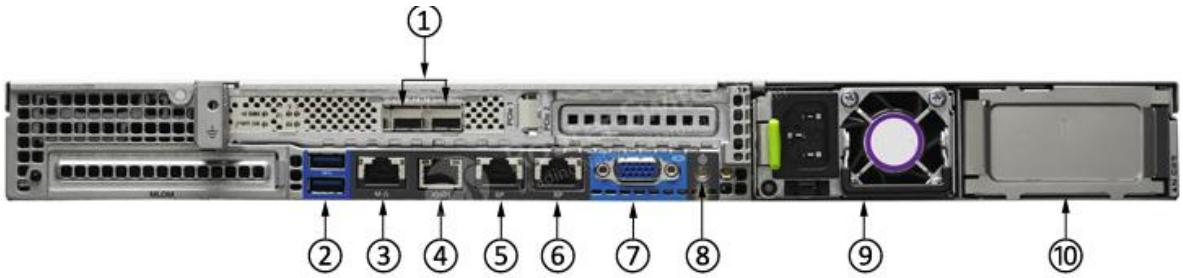
1.1 Tabla de conexión

A continuación de especifican los puertos se red asignados para la solución de ISE.

Tabla 1 Conexiones de red

Nodo	Puerto	Switch	Vlan	Puerto
WLC 1	- Port 1 (10000 Mbps)	Nexus 1	Trunk	- Port-channel 20 - Ethernet 2/4
	- Port 2 (10000 Mbps)	Nexus 2	Trunk	- Port-channel 20 - Ethernet 2/4

1.2 Definición del hardware de la controladora



①	Two 1/10 G SFP/SFP+ Ports	⑥	Redundancy Port (RP)
②	Two Type A 3.0 USB ports	⑦	VGA Connector
③	CIMC port 10/100/1000 Base-T	⑧	ID Switch and LED
④	SerialCOM Connector—Standard RS-232 Serial COM port using RJ-45 connector	⑨	Power Supply Slot
⑤	Ethernet Service Port (SP)—Management 10/100/1000 Base-T	⑩	Power Supply Slot

1.3 Definición de los puertos

Los puertos del controlador son los puertos físicos del dispositivo como se muestra en la imagen de arriba. Los siguientes son los Puertos físicos más importantes del Controlador:

- **Puerto de servicio (SP):** se utiliza para la función de inicio inicial, la recuperación del sistema y la administración fuera de banda. Si desea configurar el controlador con GUI, necesita conectar su computadora con el puerto de servicio.
- **Puerto de redundancia (RP):** este puerto se utiliza para conectar otro controlador para operaciones redundantes.
- **Puertos de distribución:** estos puertos se utilizan para todos los puntos de acceso y el tráfico de administración. Un puerto de distribución se conecta a un puerto de conmutador en modo troncal. Los controladores de la serie 4400 tienen cuatro puertos de distribución y los controladores de la serie 5500 tienen ocho puertos de distribución.
- **Puerto de la consola:** se utiliza para la administración fuera de banda, la recuperación del sistema y las funciones de arranque inicial.

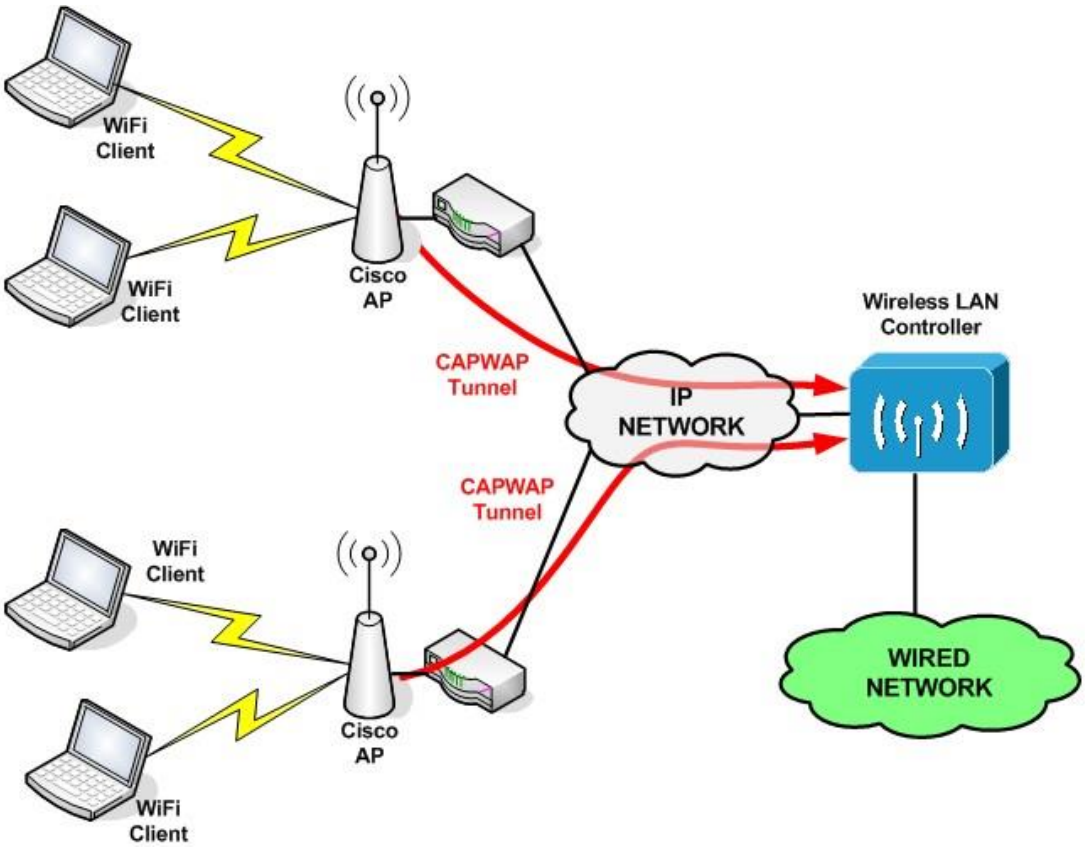
1.4 Definición de las interfaces

Las interfaces de la WLC son entidades lógicas en el dispositivo. Las siguientes son las interfaces lógicas del controlador más importantes:

- **Interfaz de Management:** se utiliza para todo el tráfico de gestión.
- **Interfaz virtual:** se utiliza para retransmitir las solicitudes DHCP del cliente, la autenticación web del cliente y para admitir la movilidad.
- **Interfaz de puerto de servicio:** vinculada al puerto de servicio y utilizada para la administración fuera de banda. La dirección IP predeterminada es 192.168.1.1. Si desea configurar el controlador por primera vez con GUI, conecte su computadora con este puerto. La computadora debe estar en la misma subred que la interfaz de servicio.
- **Interfaz dinámica:** se utiliza para conectar una VLAN a una WLAN.

1.5 Tunel Capwap

CAPWAP (Control and provisioning of Wireless Access Point) es un protocolo que hace posible vincular un punto de acceso ligero con un WLC. El protocolo CAPWAP encapsula el tráfico entre el Punto de acceso ligero y el WLC en un túnel virtual llamado túnel CAPWAP. Todo el tráfico desde el punto de acceso al WLC viaja a través de este túnel. Por lo tanto, debe tener en cuenta que en una arquitectura WiFi centralizada, todo el tráfico de los puntos de acceso termina en el controlador WLC y luego se desvía del controlador a la red cableada como se muestra en la siguiente figura:



2 Configuración inicial

A continuación, se muestra la configuración inicial del WLC 5508. Para acceder a la CLI, debe conectar su computadora al puerto de la consola del WLC con un cable de consola.

Configuración inicial del controlador de LAN inalámbrica con la CLI:

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: no

"Ingrese no para seguir las instrucciones de auto instalación"

AUTO-INSTALL: starting now. . .
System Name [Cisco_xx:xx:xx]: My_WLC
Enter Administrative User Name (24 characters max): operador
Enter Administrative Password (3 to 24 characters): *******
Re-enter Administrative Password: *******

"Ingrese el nombre de su WLC. Ingrese el nombre de usuario y la contraseña que usará para iniciar sesión en el WLC "

Service Interface IP address Configuration [static] [DHCP]: static

"Asignar una ip estática o seleccionar DHCP"

Management Interface IP Address: 172.19.12.3

Management Interface Netmask: 255.255.252.0

Management Interface Default Router: 172.19.15.254

Management Interface VLAN Identifier (0 = untagged): 110

"De forma predeterminada, la interfaz está configurada para VLAN 0, sin dirección IP y el WLC utiliza una única interfaz de administración tanto para la administración como para el tráfico CAPWAP".

Virtual Gateway IP Address: 1.1.1.1

“Se utiliza para retransmitir las solicitudes DHCP del cliente, la autenticación web del cliente y para admitir la movilidad. Este valor debe coincidir entre los grupos de movilidad".

Mobility/RF Group Name: XYZ

"Mobility / RF Group permite que múltiples WLC se agrupen en un solo grupo de controladores lógicos para permitir ajustes dinámicos de RF y roaming para clientes inalámbricos".

Network Name (SSID): TEST

Allow Static IP Addresses [YES][no]: no

"De forma predeterminada en WLC, un SSID de WLAN ya está configurado".

Configure a RADIUS Server now? [YES][no]: no

Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

“Configure los ajustes del servidor RADIUS si tiene un servidor RADIUS. Por defecto el servidor RADIUS está habilitado ".

Enter Country Code (enter ‘help’ for a list of countries) [US]: US
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

"De forma predeterminada, un WLC habilita 802.11a, 802.11b y 802.11g para todos los puntos de acceso que se asocian con él"

Configure a NTP server now? [YES] [NO]:no
Warning! No AP will come up unless the time is set.
Please see documentation for more details.

"Usted ha establecido un tiempo o un servidor NTP. Si no tiene un servidor NTP, simplemente ingrese no, inicie sesión en la GUI y configure la hora en el controlador desde allí "

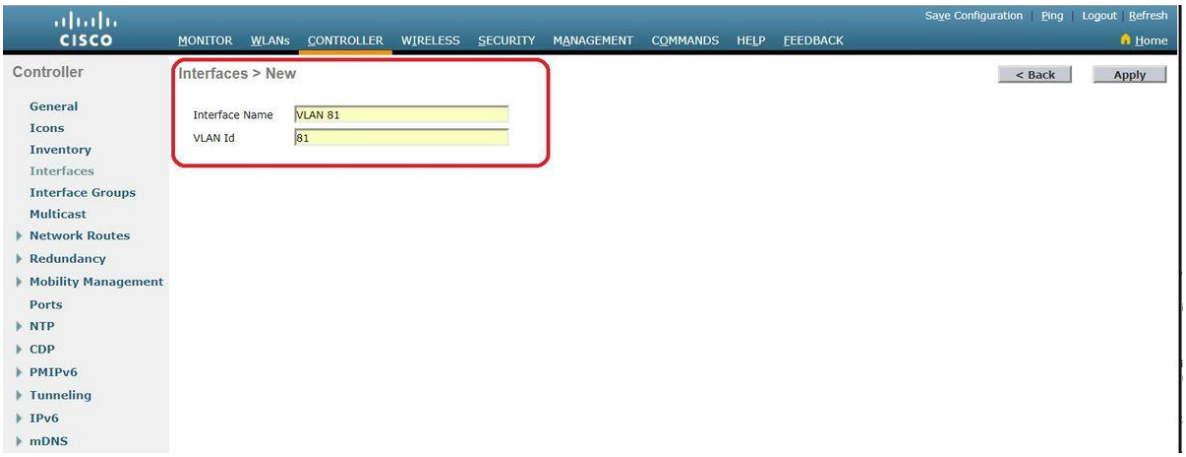
Configuration correct? If yes, system will save it and reset. [yes][NO]:yes

Configuration saved!
Resetting system with new configuration…
"Después de la configuración inicial, la WLC guarda los cambios y reinicia".

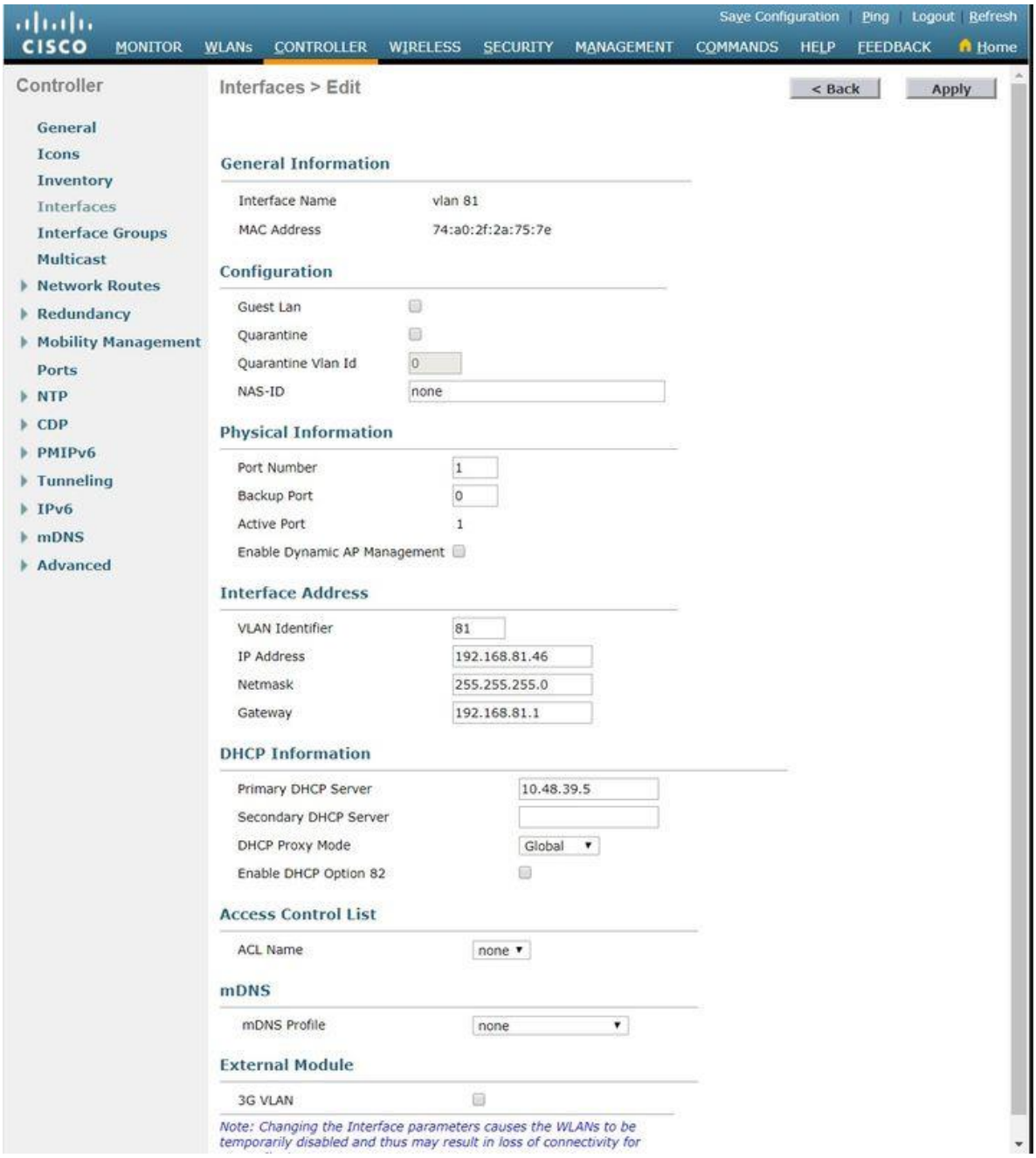
3 Creación de una interfaz vlan

Desde la GUI de WLC, elija **Controller > Interfaces**. La página de Interfaces enumera todas las interfaces que están configuradas en el WLC. Para crear una nueva interfaz dinámica, haga clic en **New**.

Ingrese el **nombre** y **Vlan ID** para la interface nueva.



Ingrese los parámetros específicos para esta interfaz VLAN. Alguno de los parámetros son **IP Address**, **Netmask**, **Gateway** y **DHCP Server IP Address**.



Nota 1: La dirección IP asignada a esta interfaz actúa como la retransmisión DHCP para que un cliente obtenga una dirección IP del servidor DHCP. Por ejemplo, cuando un cliente intenta asociarse a una WLAN / SSID asignada a esta interfaz dinámica, realiza una difusión de subred local para identificar el servidor DHCP. El controlador envía una solicitud al

servidor DHCP (o a sí mismo si es el servidor DHCP para el segmento) con la dirección IP de esta interfaz dinámica como IP de retransmisión al servidor DHCP configurado para esta interfaz. El servidor DHCP asigna una dirección IP al cliente desde el alcance DHCP configurado.

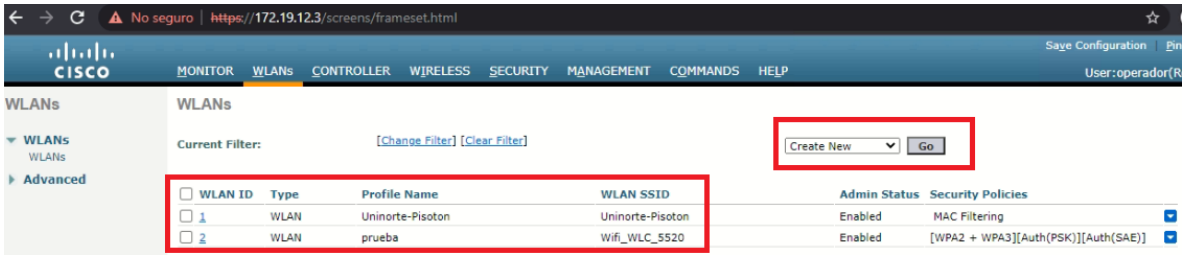
Nota2: Es obligatorio tener una dirección IP válida por razones técnicas, pero esta IP no se usará a menos que tenga el proxy DHCP o "Radius Interface Overwrite" (en la configuración de la WLAN) activada.

Nota3: El "Nombre de la interfaz" o el nombre de la Vlan es lo que puede usar como atributo del radius (airespace-interface-name) para devolver un "nombre" de la vlan en lugar de un número.

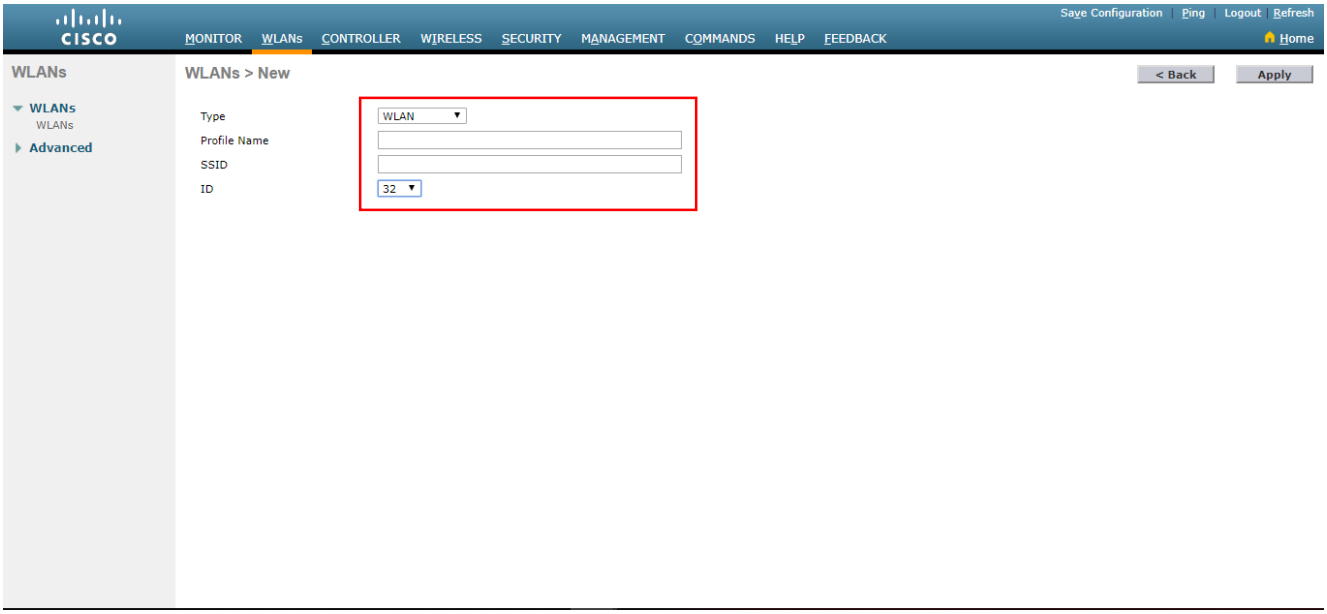
4 Creación de una WLAN

4.1 WLAN con PSK y WPA2

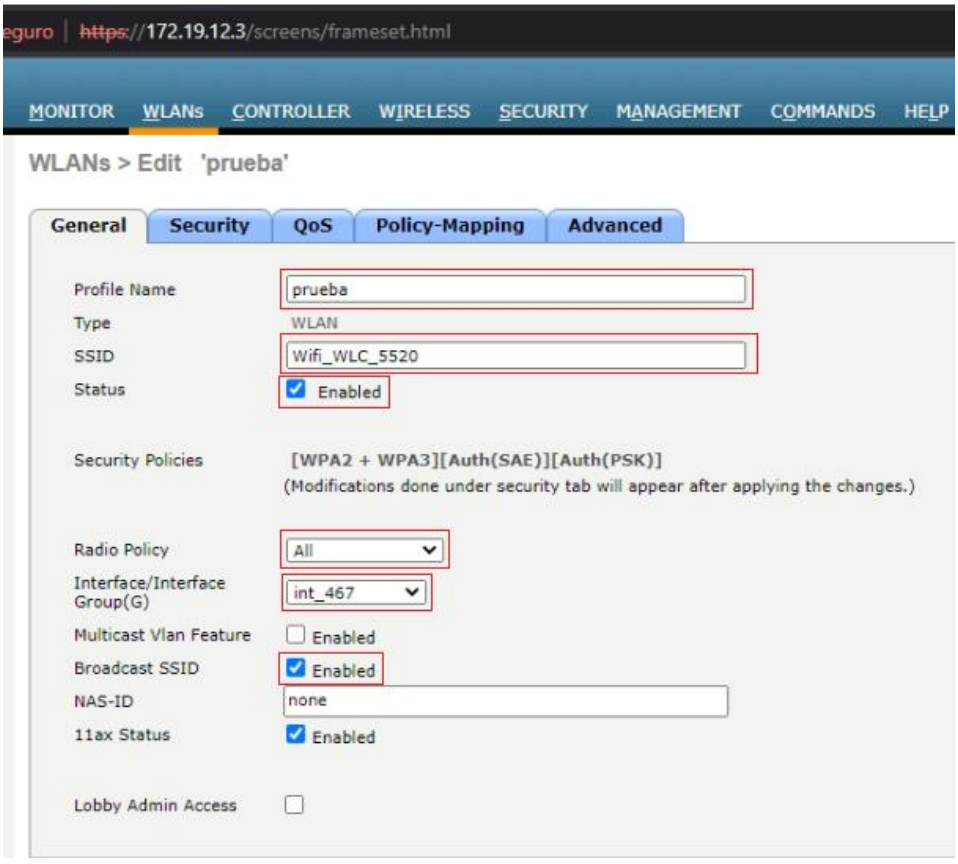
Para crear una SSID, vamos a la pestaña **WLANs** en la GUI y le damos "**Create new**" y click en **GO**.



Escogemos la opción WLAN, le damos un nombre de perfil y el nombre a la SSID que le aparecerá a los usuarios en sus dispositivos y damos click en **Apply**.



Al darle click en el botón **Apply**, nos aparecerá la siguiente pantalla:



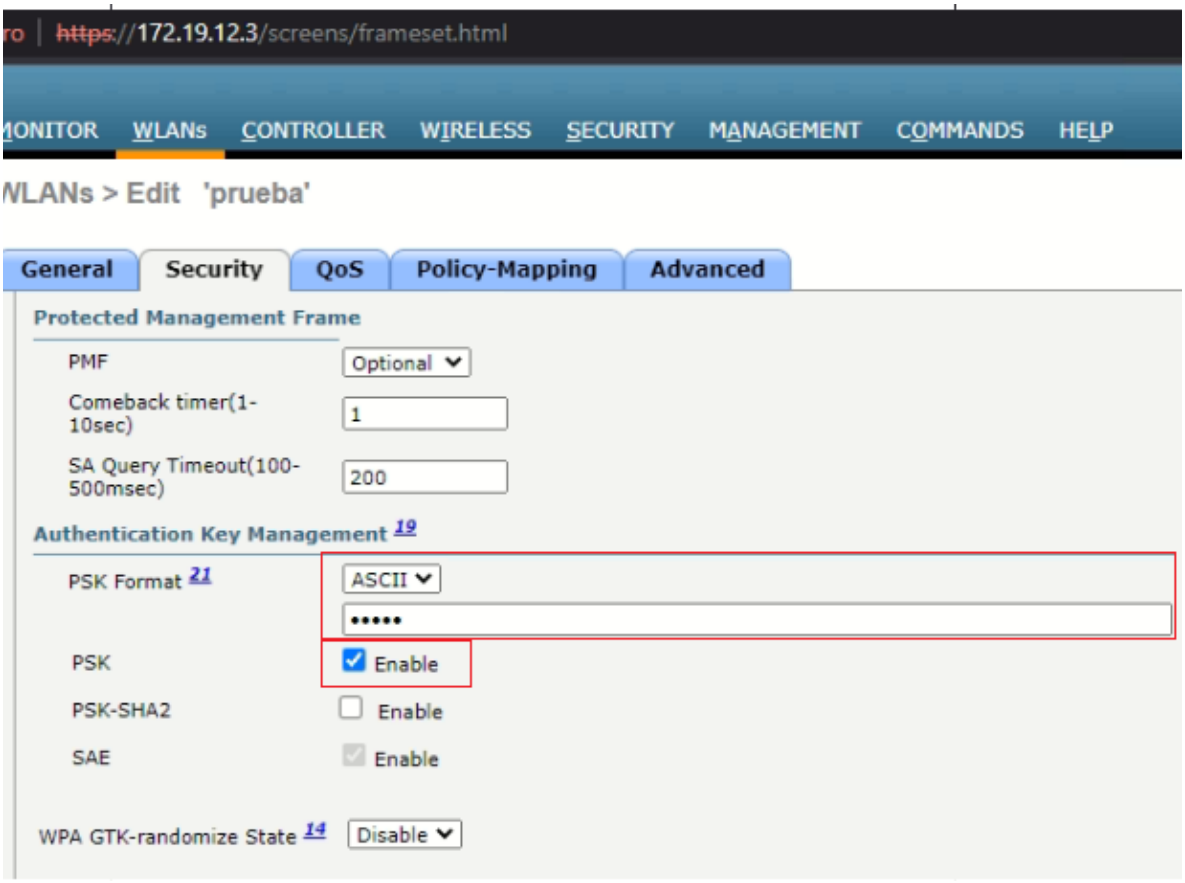
Con los datos del nombre del perfil y nombre de la SSID que nosotros previamente definimos. El **Status** debe estar habilitado para que la SSID este activa. **Radio Policy**, debe ser **All** para que acepte clientes en la banda 2.4Ghz y 5Ghz. Escogemos la interfaz previamente definida y la opción

Broadcast SSID debe estar habilitada si queremos que el usuario pueda visualizarla en su dispositivo. De esta deshabilitada, el usuario debe manualmente registrar la SSID en su dispositivo con los parámetros específicos.

Nos movemos a la pestaña de **Security** y encontraremos los siguientes parámetros.

Debemos escoger **WPA+WPA2** y seleccionar las opciones que hacen referencia a **WPA2** debido a que son las recomendaciones que hace CISCO.

Por último, el método de autenticación, que en nuestro caso será PSK o Pre-share Key.



Habilitamos la opción PSK y definimos el password en formato ASCII, que puede ser cualquier tipo de carácter que queramos definir.

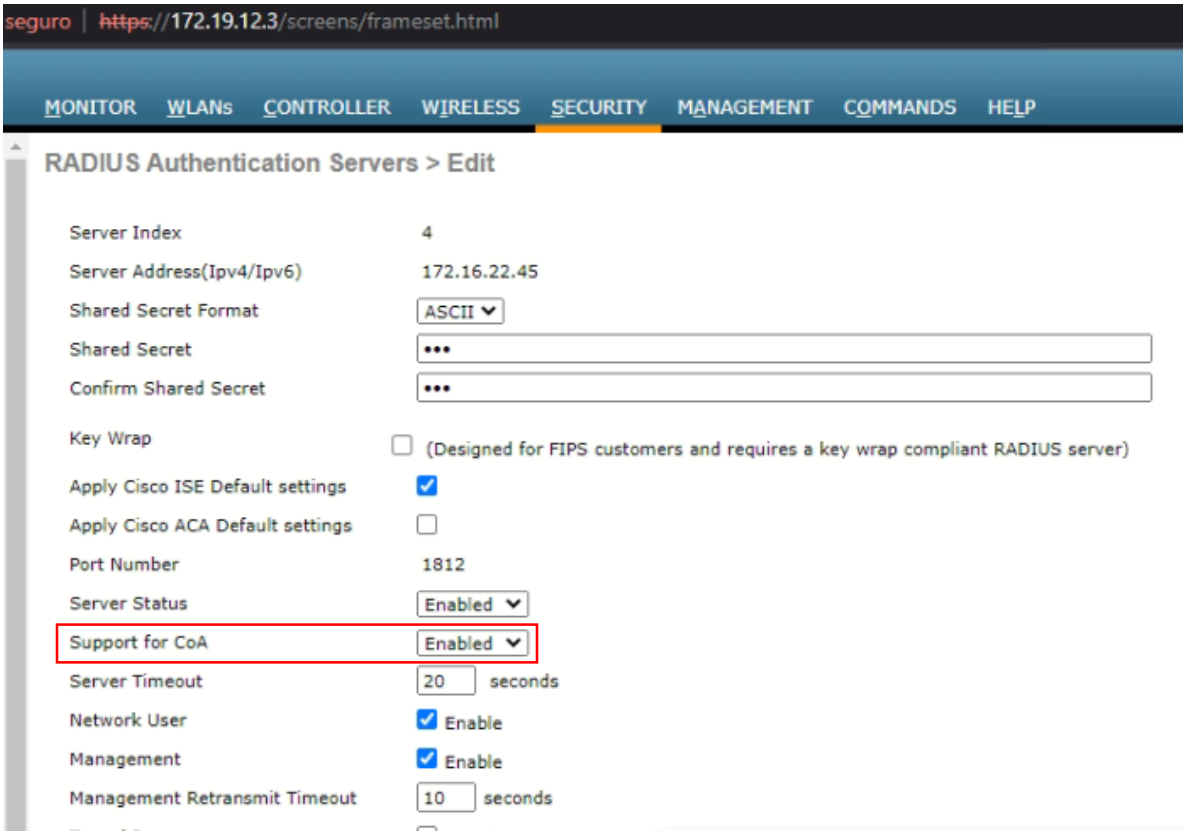
Le damos al botón **Apply** y ya tendremos nuestra nueva SSID configurada correctamente.

4.2 WLAN con Portal Cautivo

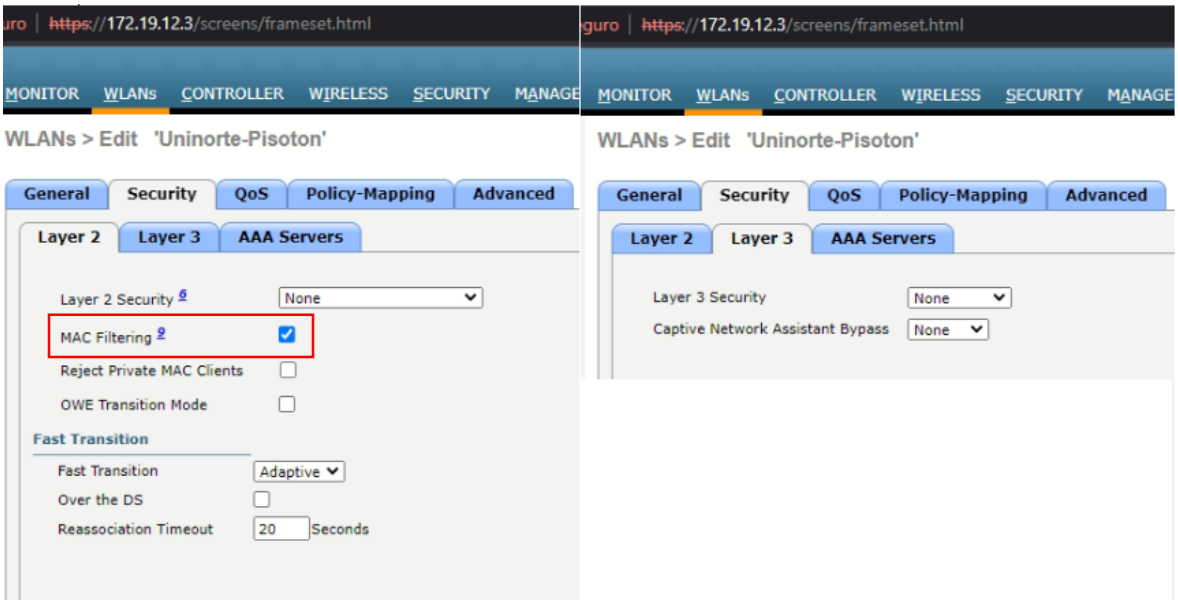
La configuración de WLC es bastante sencilla. Se utiliza un truco (igual que en los Switches) para obtener la URL de autenticación dinámica del ISE (ya que utiliza el **Change of authorization** (**CoA**), se debe crear una sesión y el ID de sesión es parte de la URL). El SSID está configurado para utilizar el filtrado de MAC. El ISE está configurado para devolver una aceptación de acceso incluso si no se encuentra la dirección MAC, de modo que envía la URL de redirección para todos los usuarios.

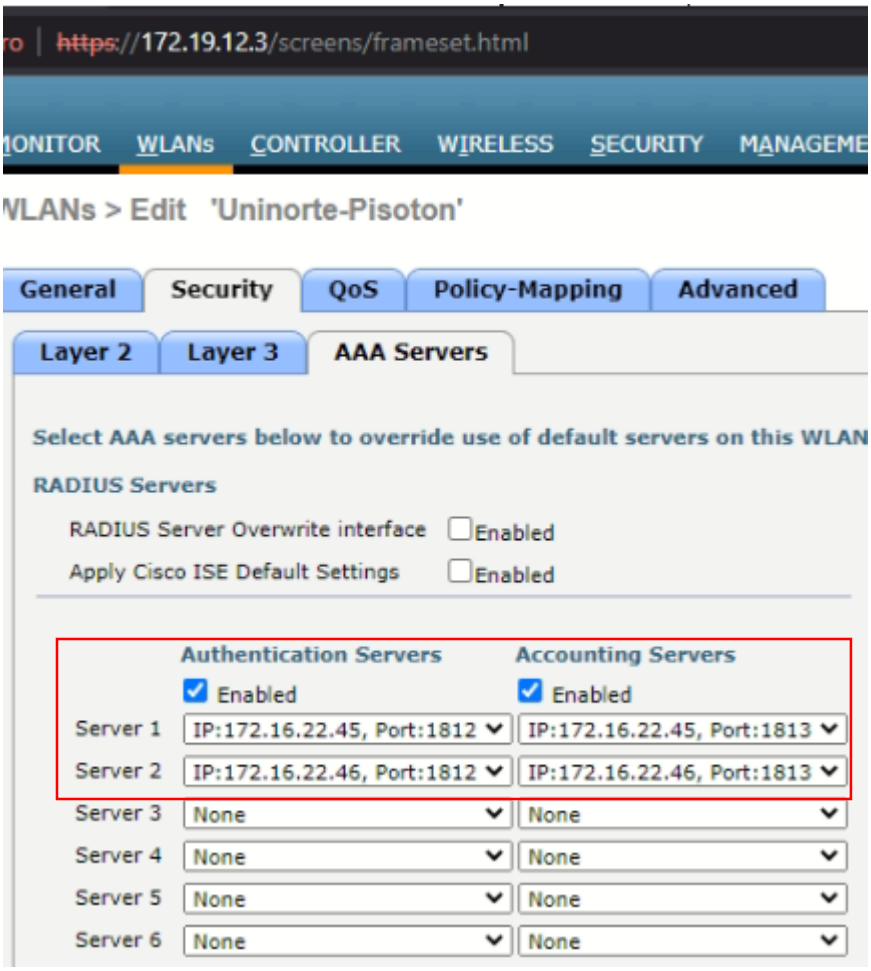
Además de esto, el **Network Admission Control** (**NAC**) de ISE y el overwrite de la autenticación, autorización y contabilidad (AAA) deben estar habilitados. El ISE NAC permite que el ISE envíe una solicitud de **CoA** que indica que el usuario ahora está autenticado y puede acceder a la red. También se utiliza para la evaluación de la postura, en cuyo caso el ISE cambia el perfil del usuario en función del resultado de la postura.

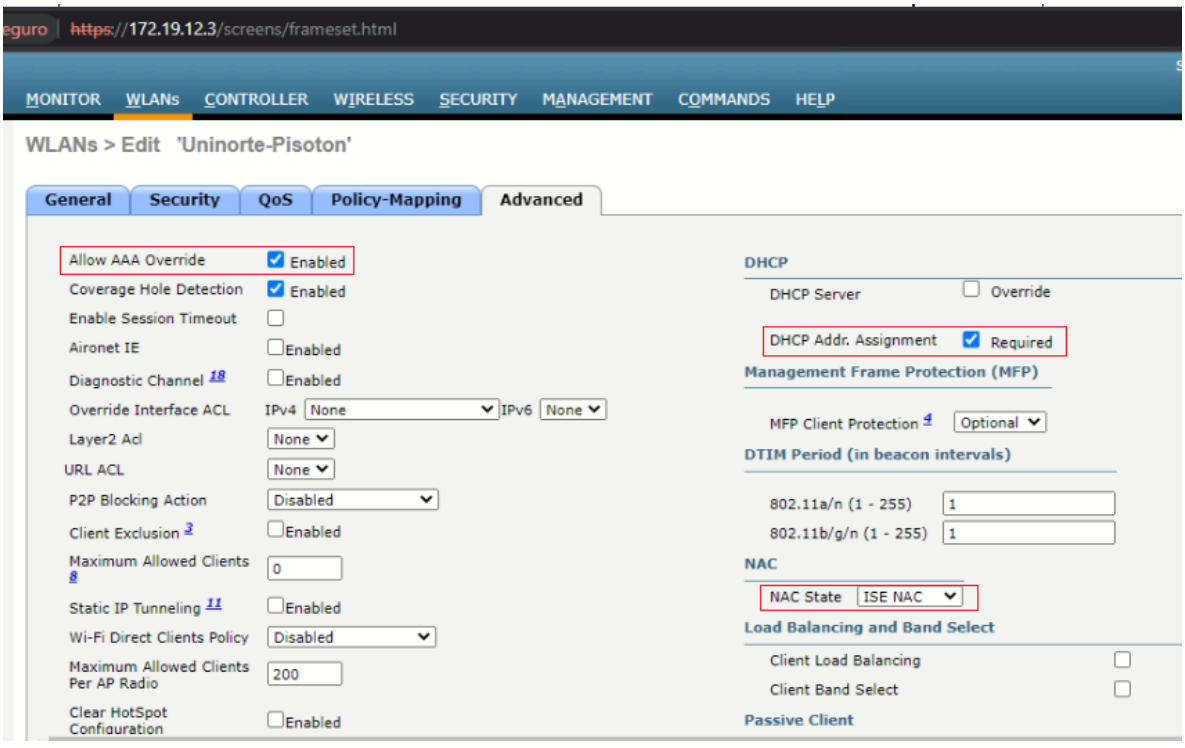
Asegúrese de que el servidor RADIUS tenga habilitado el "Soporte para CoA", que está predeterminado.



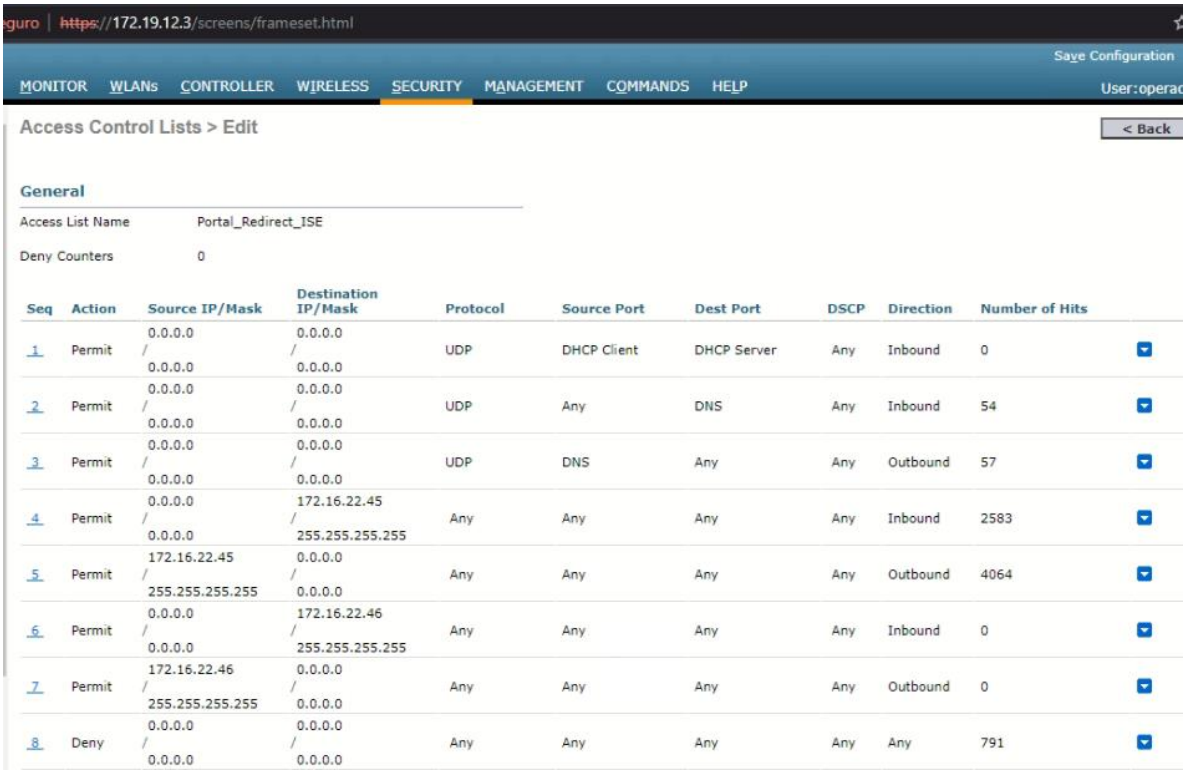
En la WLAN, la configuración debe ser la siguiente:




https://172.19.12.3/screens/frameset.html
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEME
WLANs > Edit 'Uninorte-Pisoton'
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Select AAA servers below to override use of default servers on this WLAN
RADIUS Servers
RADIUS Server Overwrite interface Enabled
Apply Cisco ISE Default Settings Enabled
Authentication Servers Enabled
Accounting Servers Enabled
Server 1 IP:172.16.22.45, Port:1812 IP:172.16.22.45, Port:1813
Server 2 IP:172.16.22.46, Port:1812 IP:172.16.22.46, Port:1813
Server 3 None None
Server 4 None None
Server 5 None None
Server 6 None None


https://172.19.12.3/screens/frameset.html
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs > Edit 'Uninorte-Pisoton'
General Security QoS Policy-Mapping Advanced
Allow AAA Override Enabled
Coverage Hole Detection Enabled
Enable Session Timeout
Aironet IE Enabled
Diagnostic Channel 18 Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion 3 Enabled
Maximum Allowed Clients 8 0
Static IP Tunneling 11 Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration Enabled
DHCP
DHCP Server Override
DHCP Addr. Assignment Required
Management Frame Protection (MFP)
MFP Client Protection 4 Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1
NAC
NAC State ISE NAC
Load Balancing and Band Select
Client Load Balancing
Client Band Select
Passive Client

Teniendo la WLAN y el Radius configurado, procedemos a crear una ACL. Se hace referencia a esta ACL en el **access-accept** del ISE y define qué tráfico debe redirigirse (denegado por la ACL) y qué tráfico no debe ser redirigido (permitido por la ACL). Aquí solo evitas el tráfico de redirección hacia el ISE. Es posible que desee ser más específico y solo evitar el tráfico hacia / desde el ISE en el puerto 8443 (portal de invitados), pero redirigir si un usuario intenta acceder al ISE en el puerto 80/443.



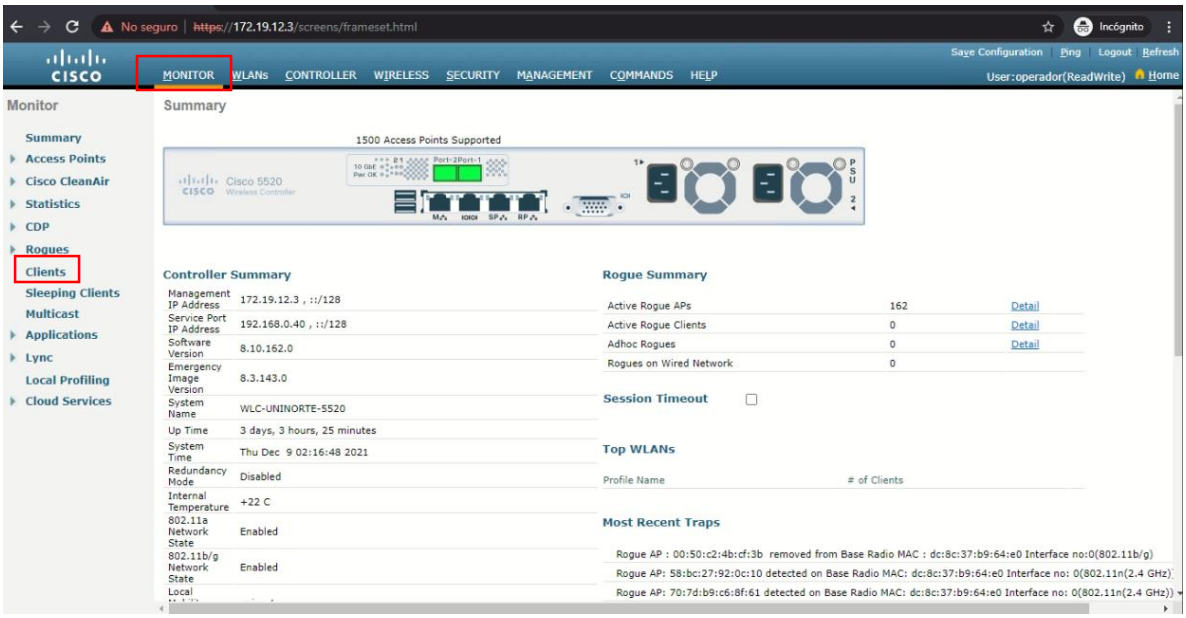
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DHCP Client	DHCP Server	Any	Inbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	54
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	57
4	Permit	0.0.0.0 / 0.0.0.0	172.16.22.45 / 255.255.255.255	Any	Any	Any	Any	Inbound	2583
5	Permit	172.16.22.45 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	4064
6	Permit	0.0.0.0 / 0.0.0.0	172.16.22.46 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
7	Permit	172.16.22.46 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
8	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	791

Con esto ya está la parte de la WLC configurada y si la parte del ISE bien configurada, los usuarios ya deberían autenticarse a través del portal.

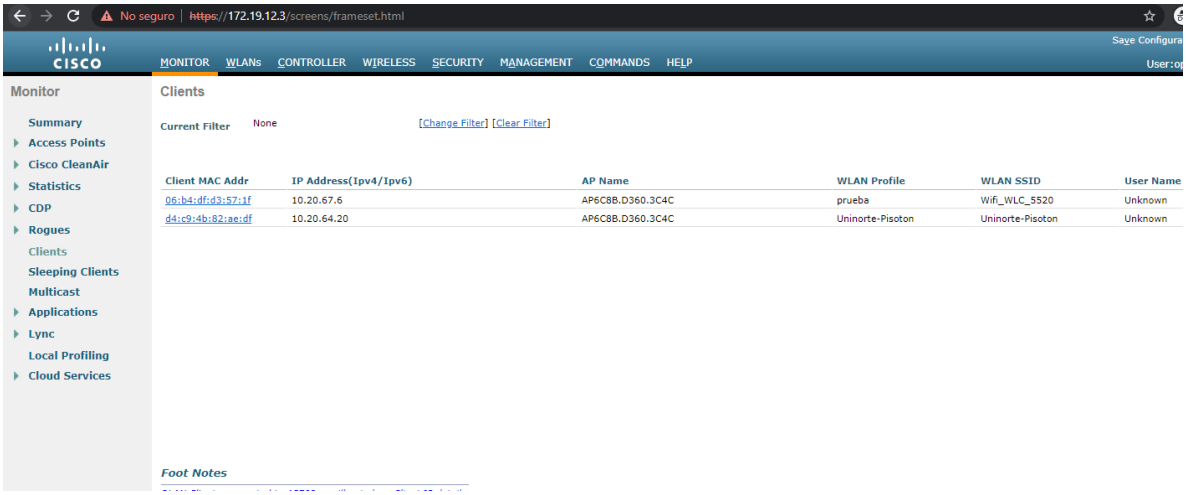
5 Revisar y eliminar usuarios conectados a la WLC

Dentro de la WLC, podemos ver todos los usuarios conectados a ella a través de los Access Points desplegados alrededor del campus.

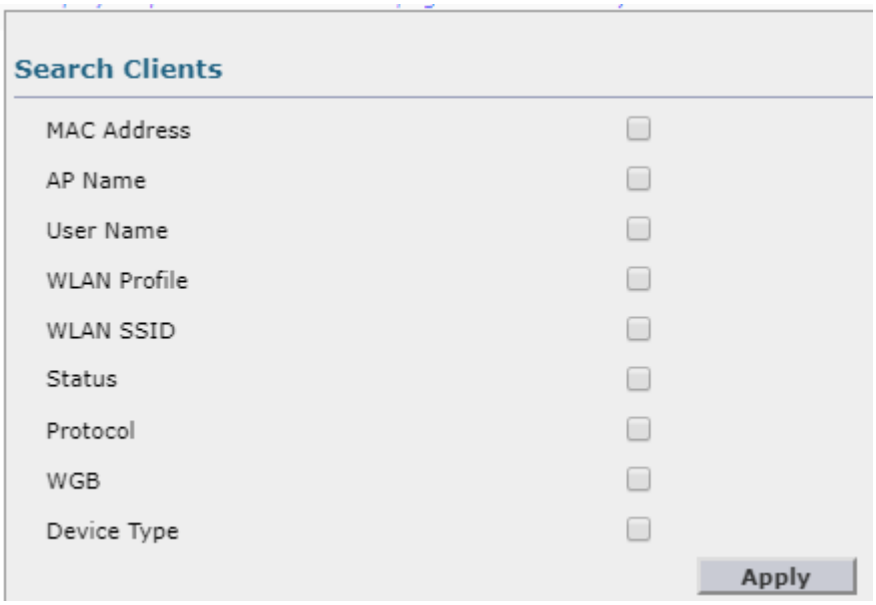
Para ver todos los usuarios conectados podemos hacerlo en la pestaña **Monitor** y seleccionando la opción, en la parte izquierda, **Clients**.



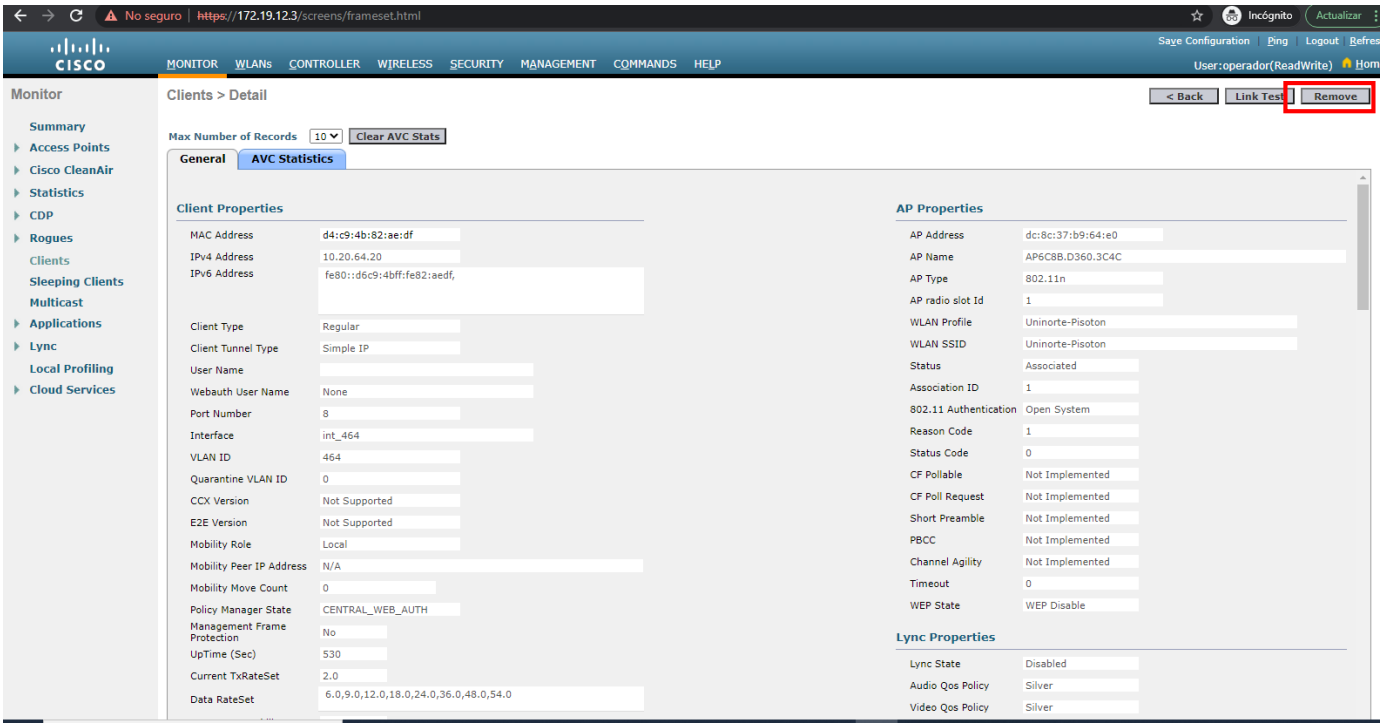
Nos aparecerá la siguiente pantalla con todos los clientes conectados:



Para eliminar un usuario, se puede buscar por medio de distintos filtros.



Después de especificar el filtro y darle aplicar, le das click al usuario que te aparece y debes tener la siguiente pantalla:



Le damos al botón en la parte superior derecha **Remove** y el usuario será desconectado de la controladora.