

Alejandro Ruiz Prior
Proyecto Integrado 2009.

**Puntos de acceso Cisco.
Configuración e instalación.**

CFGGS Administración de Sistemas Informáticos y
Redes.

Índice de contenidos.

1.- Introducción.

2.- Planteamiento inicial.

3.- Objetivos.

4.- Historia de la compañía.

5.- Características del producto utilizado.

6.- Instalación y arranque del sistema. HyperTerminal

7.- Telnet. Modos de configuración.

7.1.- Comandos principales de los modos de usuario.

8.- Parámetros básicos de configuración.

9.- Proceso personal de configuración sobre el punto de acceso.

9.1.- Configuración, problemas, y soluciones posibles.

9.2.- Resultados finales.

12.- Mejoras futuras de Cisco. Productos y tecnologías.

13.- Glosario de términos.

1.- Introducción.

La conexión a internet hoy en día nos rodea. Se ha convertido en algo esencial para nuestras vidas, y mucho más para la vida de una empresa moderna y adaptada al mundo en el que vivimos.

Cualquier persona dispone de datos personales y profesionales en la red, así como presentaciones, currículums, gráficos, estadísticas, y demás información sobre su trabajo que desee mostrar a cualquier persona a la que se dirija.

Cuando llega el turno de asistir a una empresa, o a cualquier sitio a alguna reunión, para conseguir datos que los tenga guardados en algún lugar de internet, es muy incómodo tener que estar buscando rosetas, y moviéndose para adaptarse al lugar de la roseta. Por no hablar de que cuando varias personas están conectadas a una red así, si por cualquier caso tuvieran que hacer un uso intensivo de la red, el resto de la empresa, y sus trabajadores lo notarían, relentizando su trabajo, y por tanto, el rendimiento de la empresa.

Cuando entré en Grupo AMS, me comentaron la solución que le querían dar a todo esto. Lo primero era crear la red wifi en el edificio, y que ninguna de las 4 plantas se quedara sin cobertura. Y luego, separar el tráfico que recibirían de visitas, clientes, y entrevistados, del que habitualmente utilizan los empleados durante su jornada de trabajo.

2.- Planteamiento inicial.

Para obtener el mejor rendimiento posible de la futura red wifi, se confía en Cisco y en sus puntos de acceso por las varias opciones de configuración que ofrecen, y sobre todo, porque con estos puntos de acceso, se dividiría el tráfico de la red directamente en 2 redes, una para trabajadores, y otra para la gente externa a la empresa, es decir, de la red de la empresa, a través de la red wifi saldrían 2 redes virtuales, las llamadas VLAN.

Para que ningún rincón se quede sin cobertura wifi, se instalarían 4 puntos de acceso por todo el edificio, uno por cada planta. Se recomienda que no esté a menos de 20 cms de una persona, por lo que se colocan cerca del techo, en una parte relativamente céntrica de la planta.

Otra ventaja que se puede sacar de estos puntos de acceso es que si está conectado mientras cambia de planta, se conectará automáticamente al punto de acceso de la planta nueva en la que se encuentre.

3.- Objetivos.

El principal objetivo de este proyecto es conocer los sistemas de Cisco, ya que en mi caso, durante el curso de primero no se impartió nada sobre este tema.

4.- Historia de la compañía.

Cisco fue fundada en el año 1984 por un grupo pequeño de científicos de la Universidad de Stanford. Desde los inicios de la compañía, los ingenieros de Cisco han sido líderes en el desarrollo de tecnologías de conectividad basadas en el Protocolo de Internet (IP). Actualmente, con más de 47.000 empleados en todo el mundo, esa tradición de innovación continúa en productos y soluciones líderes en la industria, en las áreas principales de la compañía de routing y switching, así como en tecnologías avanzadas tales como: Comunicaciones IP, LAN Inalámbrica, Conectividad en el Hogar, Servicios de Aplicación de Red, Seguridad de Red, Redes de Area de Almacenamiento, Sistemas de Video.

Su nombre fue elegido porque desde la ventana del laboratorio donde empezaron todo, se veía un cartel de la ciudad de San Francisco, solo que un árbol tapaba parte del cartel, y lo que finalmente aparecía en el cartel era “cisco”.

Cisco se mueve tanto en hardware como en software. Tras ser los creadores del primer router, y de luego abrir el abanico hasta varios productos más como switchs o puntos de acceso. Crean el software para la configuración y gestión de sus productos. Un software que, todo hay que decirlo, es propietario y de código cerrado.

Con todo esto Cisco es, hoy en día, líder mundial en servicios de soluciones de red e infraestructuras para internet.

Últimamente, Cisco ha sufrido un pequeño cambio de imagen, más estilizados, a juego con sus últimas líneas de productos.



5.- Características del producto.

Para realizar la instalación de la red wifi, se han adquirido cuatro puntos de acceso Cisco Aironet 1130 AG.

Este modelo de Cisco es un punto de acceso con perfil bajo para la clase empresarial, con antenas integradas para una fácil integración en oficinas y entornos similares.

Proporciona funciones de alta capacidad, de alta seguridad, de clase empresarial en un punto de acceso discreto, con un atractivo diseño, ideal para oficinas, ofreciendo acceso inalámbrico a Internet con el menor coste total de propiedad.

Incluye las radios 802.11a y 802.11g.

Tiene una RAM de 32MB y una memoria flash de 16MB.

Alcance en interior: 137m.

Alcance en exterior: 290m.

Protocolo de conexión de datos: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g.

Protocolo de gestión de normas: SNMP, Telnet, HTTPS.

Cumplimiento de normas: IEEE 802.3, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, Wi-Fi certified.



6.- Instalación y arranque del sistema. HyperTerminal.

Cuando coges el punto de acceso, notarás que aparentemente no tienen ninguna entrada para conexiones ni nada, cuidando al máximo el diseño.

Para conectar los cables, será necesario deslizar la tapa como se ve en la imagen.



La disposición de los cables queda así de izquierda a derecha:

- Cable de corriente
- Cable de red
- Cable de consola

A la derecha del cable de consola está el botón de reset, y a continuación las luces de estado del punto de acceso.

El otro extremo del cable consola es un conector de 9 pines, que se conectará al ordenador desde el que queremos configurar el dispositivo. El cable de red debe de ir conectado a un servidor DHCP, ya que el punto de acceso no deja que se configure en modo local desde un principio, y será el servidor DHCP el que nos dé una ip para configurarlo.

El punto de acceso no tiene botón de apagar o encender ni nada, por tanto, en el momento en el que se enchufe, arrancará el dispositivo. Antes de encenderlo, configuramos HyperTerminal, para que nos muestre el registro del arranque, en el que, entre otras cosas, nos muestra la ip que coge.

La configuración de los parámetros de conexión para HyperTerminal por el puerto COM1 sería esta:

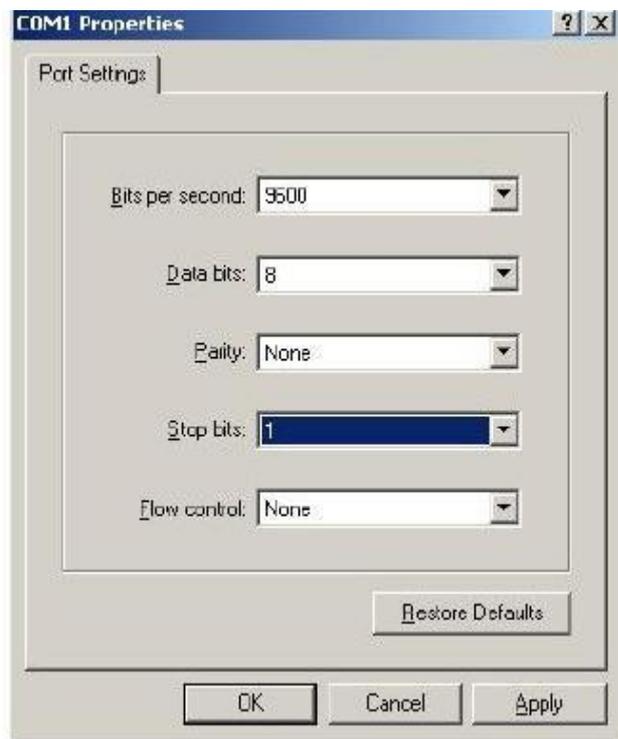
Bits por segundo: 9600

Bits de datos: 8

Bits de paridad: Ninguno

Bits de parada: 1

Control de flujo: Ninguno



Esto es lo que muestra:

```
Xmodem file system is available.
flashfs[0]: 150 files, 7 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 6098944
flashfs[0]: Bytes available: 9900032
flashfs[0]: flashfs fsck took 31 seconds.
Base ethernet MAC Address: 00:1d:a1:ef:4f:a8
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
ethernet link up, 100 mbps, full-duplex TIPO DE CABLE ENCHUFADO
Ethernet port 0 initialized: link is up EL CABLE DE RED ESTÁ CONECTADO
Loading "flash:/c1130-k9w7-mx.124-10b.JA/c1130-k9w7-mx.124-10b.JA"...
#####
#####
#####
#####
#####
File "flash:/c1130-k9w7-mx.124-10b.JA/c1130-k9w7-mx.124-10b.JA" uncompressed and installed, entry point: 0x3000
executing...
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software – Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C1130 Software (C1130-K9W7-M), Version 12.4(10b)JA, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 24-Oct-07 15:17 by prod_rel_team
Image text-base: 0x00003000, data-base: 0x00861260

Initializing flashfs...

```
flashfs[1]: 150 files, 7 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 15998976
flashfs[1]: Bytes used: 6098944
flashfs[1]: Bytes available: 9900032
flashfs[1]: flashfs fsck took 4 seconds.
flashfs[1]: Initialization complete....done Initializing flashfs.
Radio 1 A506 7100 E8000000 A0000000 80000000 3
Radio 1 A506 6700 E8000100 A0040000 80010000 2
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to toexport@cisco.com.

INFORMACIÓN DEL PUNTO DE ACCESO

cisco AIR-AP1131AG-E-K9 (PowerPCelvis) processor (revision A0) with 24566K/8192K bytes of memory.
Processor board ID FCZ1151Q1JU
PowerPCelvis CPU at 262Mhz, revision number 0x0950
Last reset from power-on
1 FastEthernet interface
2 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.

```
Base ethernet MAC Address: 00:1D:A1:EF:4F:A8
Part Number : 73-8962-12
PCA Assembly Number : 800-24818-11
PCA Revision Number : B0
PCB Serial Number : FOC114909XX
Top Assembly Part Number : 800-29230-01
Top Assembly Serial Number : FCZ1151Q1JU
Top Revision Number : A0
Product/Model Number : AIR-AP1131AG-E-K9
```

Press RETURN to get started! **PRESIONANDO INTRO, SE INICIA EL SERVICIO DEL PUNTO DE ACCESO**

```
*Mar 1 00:00:05.574: %SOAP_FIPS-2-SELF_TEST_IOS_SUCCESS: IOS crypto FIPS self test passed
*Mar 1 00:00:07.181: %SOAP_FIPS-2-SELF_TEST_RAD_SUCCESS: RADIO crypto FIPS self test passed on interface Dot11Radio 0
*Mar 1 00:00:08.755: %SOAP_FIPS-2-SELF_TEST_RAD_SUCCESS: RADIO crypto FIPS self test passed on interface Dot11Radio 1
*Mar 1 00:00:10.925: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
*Mar 1 00:00:11.411: %SYS-5-CONFIG_I: Configured from memory by console
*Mar 1 00:00:11.414: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C1130 Software (C1130-K9W7-M), Version 12.4(10b)JA, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 24-Oct-07 15:17 by prod_rel_team
```

*Mar 1 00:00:11.414: %SNMP-5-COLDSTART: SNMP agent on host ap_cisco1 is undergoing a cold start
*Mar 1 00:00:11.445: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset
*Mar 1 00:00:11.445: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 1 00:00:11.445: %CDP_PD-4-POWER_OK: Full power - AC_ADAPTOR inline power source
*Mar 1 00:00:11.449: %DOT11-4-NO_SSID_VLAN: No SSID with VLAN configured. Dot11Radio1 not started.
*Mar 1 00:00:11.482: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

*Mar 1 00:00:11.484: %DOT11-4-NO_SSID_VLAN: No SSID with VLAN configured. Dot11Radio1 not started.
*Mar 1 00:00:11.485: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down
*Mar 1 00:00:11.490: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 1 00:00:11.512: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

*Mar 1 00:00:11.925: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
*Mar 1 00:00:12.344: %LINEPROTO-5-UPDOWN: Line protocol on Interface BV11, changed state to up
*Mar 1 00:00:12.445: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to down
*Mar 1 00:00:12.445: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
*Mar 1 00:00:21.426: %DHCP-6-ADDRESS_ASSIGN: Interface BV11 assigned DHCP address 192.168.39.94, mask 255.255.255.0, hostname ap_cisco1
FINALMENTE, NOS DICE LA IP ASIGNADA POR EL SERVIDOR DHCP, Y EL NOMBRE DEL PUNTO DE ACCESO.

HyperTerminal sólo muestra datos, no recibe ningún parámetro, para eso, sería necesario utilizar la consola web, o un Telnet.

7.- Telnet. Modos de configuración.

Para enviar comandos al punto de acceso, necesitamos una conexión por telnet.

Para abrir la conexión, necesitamos que el punto de acceso ya tenga una ip asignada, y tecleamos esto:

```
ap_cisco> o 192.168.1.11(ip asignada)
```

Por defecto, el usuario y password es **Cisco**. Desde ese momento, estamos en modo EXEC usuario. ¿Eso qué significa? A continuación tienes las definiciones de los tres modos de configuración del punto de acceso bajo la línea de comandos.

Modo EXEC Usuario

Este modo solo permite ver información limitada de la configuración del router y no permite modificación alguna de ésta. El símbolo > en el prompt indica que usted se encuentra en modo de usuario.

Modo EXEC Privilegiado

Este modo permite ver en detalle la configuración del router para hacer diagnósticos y pruebas. También permite trabajar con los archivos de configuración del router (Flash - NVRAM).

Modo de Configuración Global

Este modo permite la configuración básica de router y permite el acceso a submodos de configuración específicos. Este es el principal para ajustar todos los parámetros de la configuración de las VLAN, los SSID, y todo lo referente a cambios para el rendimiento del punto de acceso.

A continuación, una muestra sobre como cambiar de un usuario a otro en línea de comandos:

```
ap_cisco>
ap_cisco> enable (pasa al Modo Exec Privilegiado)
ap_cisco#
ap_cisco# exit (vuelve a al Modo Exec Usuario)
ap_cisco> enable
ap_cisco#
ap_cisco# configure terminal (pasa al Modo Configuración Global)
ap_cisco(config)#
ap_cisco(config)# exit (vuelve al Modo Exec Privilegiado)
ap_cisco#
```

7.1.- Comandos principales de los modos de usuario.

Modo EXEC Usuario

<1-99> -> Acceder a número de sesión
access-enable -> Crear una lista de acceso temporal
clear -> Reiniciar funciones
connect -> Abrir una conexión del terminal
crypto -> Encryption related commands.
disable -> Quitar los comandos privilegiados
disconnect -> Desconectar de la conexión de red existente
dot11 -> Comandos IEEE 802.11
enable -> Accede a modo privilegiado
exit -> Sale del modo EXEC
help -> Ayuda
led -> Funciones led
lock -> Bloquear el terminal
login -> Acceder con un usuario particular
logout -> Cerrar sesión
name-connection -> Nombra una conexión de red existente
ping -> Hace ping
radius -> Comandos EXEC de radius
release -> Lanzar un recurso
renew -> Renovar un recurso
resume -> Reanudar una conexión de red activa

save -> Guarda la pila de raise_interrupt_level
set -> Ajuste de parámetros del sistema(no de configuración)
show -> Mostrar la información del sistema cuando está corriendo
ssh -> Abre una conexión SSH
sysstat -> Muestra información sobre las líneas del terminal
telnet -> Abrir una conexión telnet
terminal -> Establecer parámetros de la línea del terminal
traceroute -> Traza la ruta al destino
tunnel -> Abrir una conexión túnel
where-> Conexiones de lista activa

Modo EXEC Privilegiado

<1-99> -> Acceder a número de sesión
access-enable -> Crear una lista de acceso temporal
access-template -> Crear una lista de acceso temporal
archive -> Gestionar archivos
cd -> Cambiar el directorio actual
clear -> Reiniciar funciones
clock -> Gestionar el reloj
configure -> Entra en modo configuración global
connect -> Abrir una conexión del terminal
copy -> Copiar
crypto -> Cifrado de comandos relacionados
debug -> Funciones de depuración
delete -> Eliminar
dir -> Listar ficheros en un directorio
disable -> Quitar los comandos privilegiados
disconnect -> Desconectar de la conexión de red existente
dot11 -> Comandos IEEE 802.11
dot1x -> Comandos Exec IEEE 802.11X
enable -> Accede a modo privilegiado
erase -> Borrar un sistema de ficheros
exit -> Sale del modo EXEC
format -> Formatea un sistema de ficheros
fsck -> Ejecuta fsck sobre un sistema de ficheros

help -> Ayuda
led -> Funciones led
lock -> Bloquear el terminal
login -> Acceder con un usuario particular
logout -> Cerrar sesión
mkdir -> Crear nuevo directorio
monitor -> Monitoriza eventos del sistema
more -> Muestra el contenido de una fila
name-connection -> Nombra una conexión de red existente
no -> Desactiva las funciones de depuración
ping -> Hace ping
pwd -> Muestra el directorio de trabajo actual
radius -> Comandos EXEC de radius
release -> Lanzar un recurso
reload -> Halt and perform a cold restart
rename -> Renombra un fichero
renew -> Renovar un recurso
resume -> Reanudar una conexión de red activa
rmdir -> Borra un directorio existente
rsh -> Ejecuta comando remotamente
save -> Guarda la pila de raise_interrupt_level
send -> Manda un mensaje a otro tty
set -> Ajuste de parámetros del sistema(no de configuración)
show -> Mostrar la información del sistema cuando está corriendo
ssh -> Abre una conexión SSH
sysstat -> Muestra información sobre las líneas del terminal
telnet -> Abrir una conexión telnet
terminal -> Establecer parámetros de la línea del terminal
test -> Prueba de subsistemas, la memoria y las interfaces
traceroute -> Traza la ruta al destino
tunnel -> Abre una conexión tunel
undebg -> Desactiva funciones de depuración
upgrade -> Actualiza el software
verify -> Verifica un fichero
where -> Lista las conexiones activas

write -> Escribir funcionamiento a la configuración de memoria, red, o terminales

Modo de Configuración Global

aaa -> Autenticación, Autorización y Contabilización.

access-list -> Añadir una lista de acceso de entrada

alias -> Crear alias

archive -> Archiva la configuración

arp -> Establece una entrada ARP estática

banner -> Define a login banner

boot -> Comandos de arranque

bridge -> Grupo puente

buffers -> Ajusta los parámetros del búfer del sistema

call -> Configura los parámetros de llamada

cdp -> Global CDP configuration subcommands

class-map -> Configure QoS Class Map

clock -> Configura el reloj

configuration -> Acceso a la configuración

crypto -> Módulo de encriptación

default -> Establece el comando a su estado por defecto

default-value -> Valor de bits por carácter por defecto

define -> Interfaz serie de definiciones de macros

do -> Ejecitar comandos EXEC en modo configuración

dot11 -> Comandos de configuración de IEEE 802.11

dot1x -> Comandos de configuración de IEEE 802.1X

downward-compatible-config -> Genera una configuración compatible con software viejo

eap -> Comandos de configuración de EAP

enable -> Modifica los parámetros de la password de enable

end -> Finaliza el modo de configuración

exception -> Manejo de excepciones

exit -> Sale del modo de configuración

file -> Ajusta parámetros del sistema de ficheros

help -> Ayuda

hostname -> Establece un nombre a la red del sistema

iapp -> Comandos de configuración de IAPP

interface -> Selecciona una interfaz a configurar

ip -> Subcomandos de configuración de IP

led -> Ajusted de LED

li-view -> Vista LI

line -> Configura una línea del terminal

logging -> Modify message logging facilities

login -> Habilitar la utilización de loguearse

map-class -> Configurar las clases de mapa estáticas

map-listv -> Configurar las listas de mapa estáticas

memory -> Configuración de la gestión de la memoria

monitor -> Monitoriza eventos del sistema

no -> Rechazar un comando o ajustarlo por defecto

parser -> COnfigurar el analizador

policy-map -> Configurar las políticas QoS

power -> Configuración de la alimentación

privilege -> Parámetros de los comandos de privilegio

process -> Configurar procesos

process-max-time -> Máximo tiempo para el proceso antes de abandonar voluntariamente el procesador

regexp -> Comandos de regexp

resource -> Configurar el ERM

scheduler -> Parámetros de programador

service -> Modificar servicios basados en el uso de la red

snmp -> Modify non engine SNMP parameters

snmp-server -> Modify SNMP engine parameters

sntp -> Configurar SNTP

subscriber-policy -> Políticas de suscriptor

table-map -> Configurar table-map

tacacs-server -> Modificar parámetros de consulta a TACACS template -> Selecciona una plantilla para configurar

tftp-server -> Proporciona servicio TFTP para solicitudes netload

time-range -> Definir rango de tiempo de las entradas

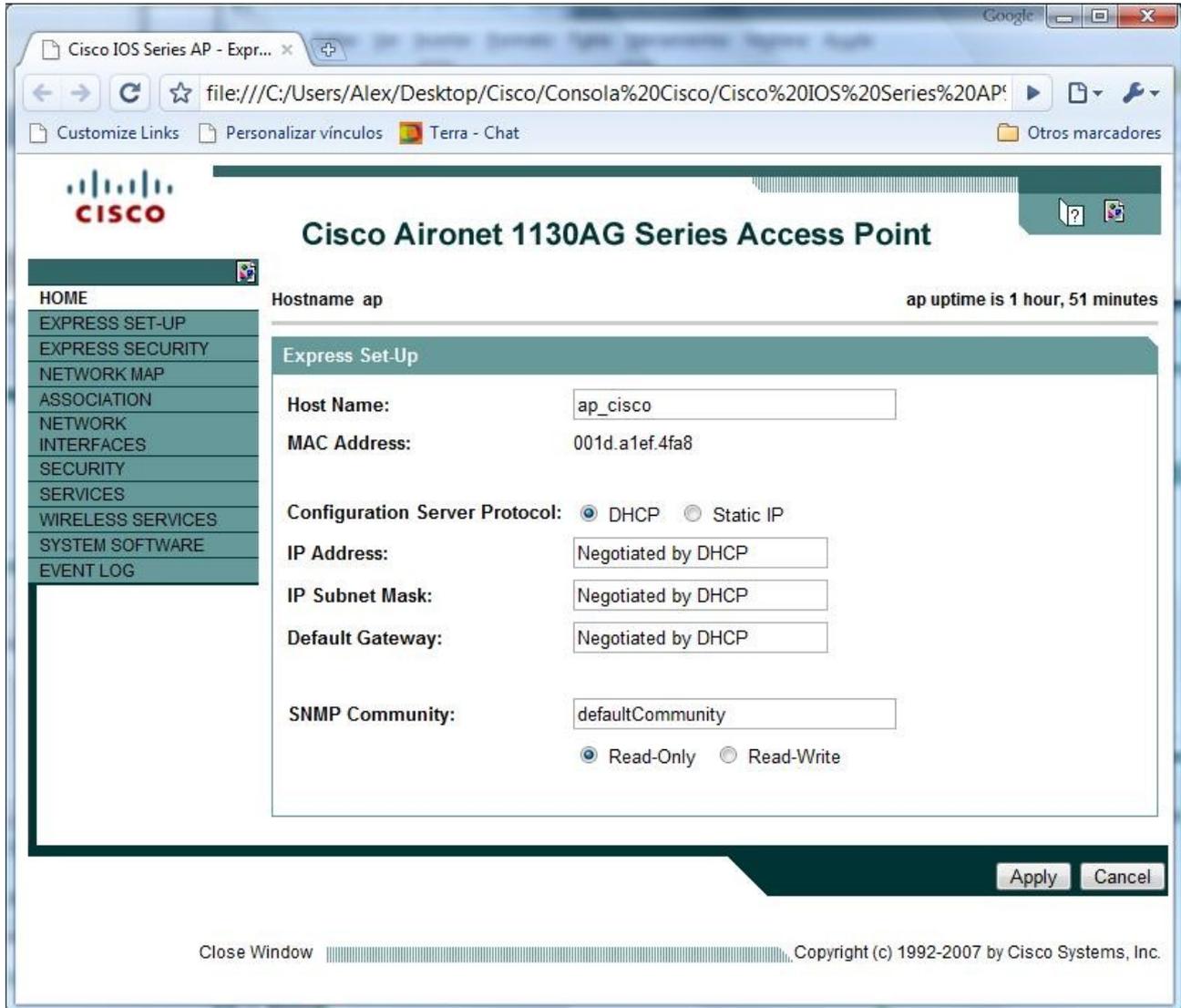
username -> Establece un nombre de usuario para la autenticación

vlan -> Comandos de VLAN

wlccp -> Habilitar WLCCP

workgroup-bridge -> Configurar comandos de puente de grupo de trabajo IEEE 802.11

8.- Parámetros básicos de configuración



Desde esta página cambias el nombre del punto de acceso, para distinguirlo, por ejemplo, en el caso de configurarlo mediante línea de comandos. Se puede observar que este tiene la configuración por DHCP, y no aparece la ip.

Si marcas la opción de ip estática, lo puedes cambiar manualmente quedando como en la siguiente imagen.



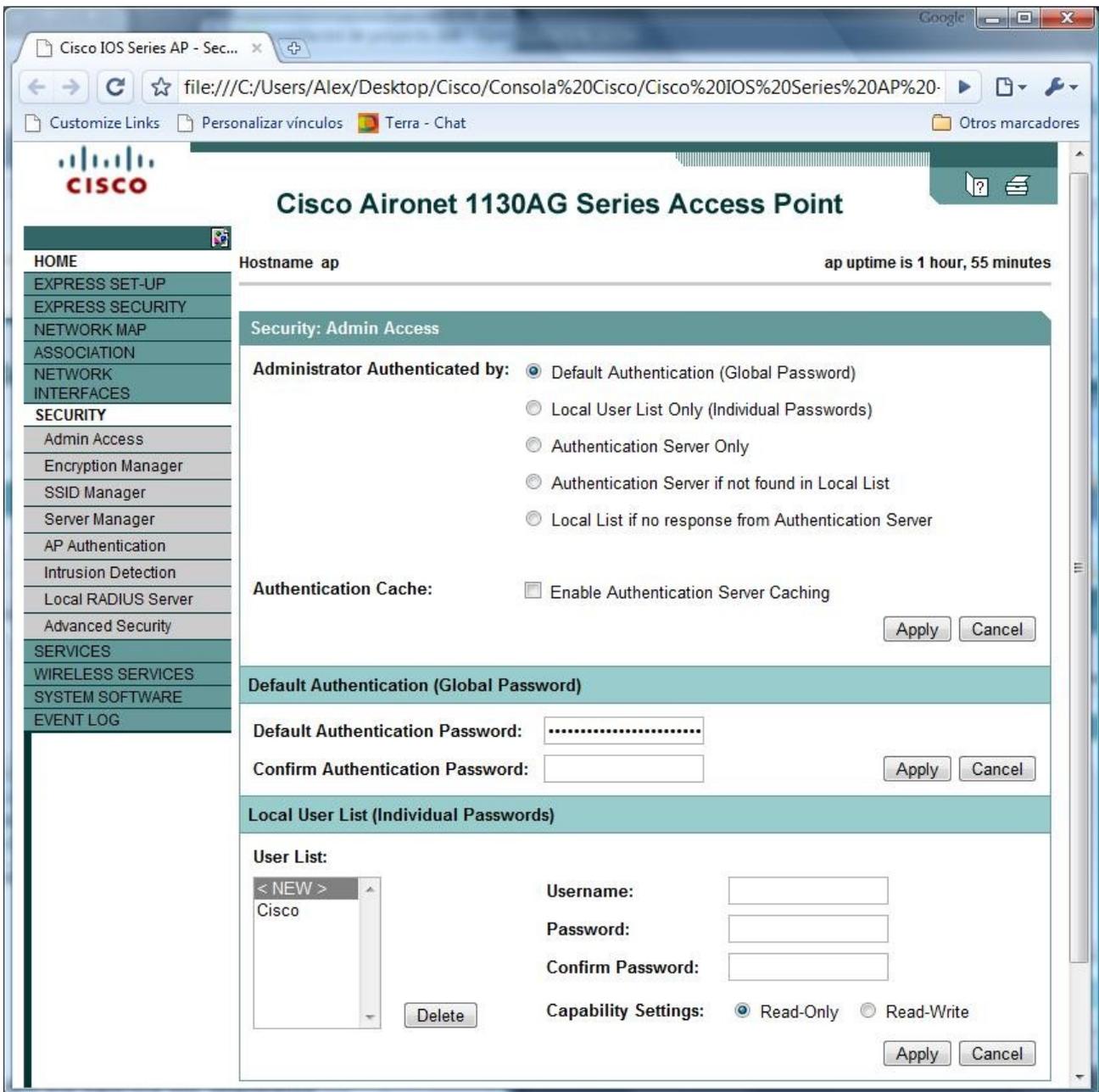
Esto lo puedes cambiar mediante telnet con el siguiente comando:

```
ap_cisco(config)# hostname CISCO  
CISCO(config)#
```

O si quieres cambiar por ejemplo la contraseña de inicio, hay que teclear lo siguiente, accediendo primero como modo de configuración global:

```
ap_cisco1(config)# line console 0 (accede al sector del punto de acceso en el que cambia la  
contraseña)  
ap_cisco1(config-line)# password contraseña  
ap_cisco1(config-line)# login  
ap_cisco1(config-line)# exit
```

Si lo quieres cambiar por la consola web, tienes que irte a las opciones de seguridad, y dentro de ahí, a Admin Access.



Por aquí además, tiene la opción de gestionar varios usuarios, así como los permisos de cada uno.

9.- Proceso personal de configuración sobre el punto de acceso.

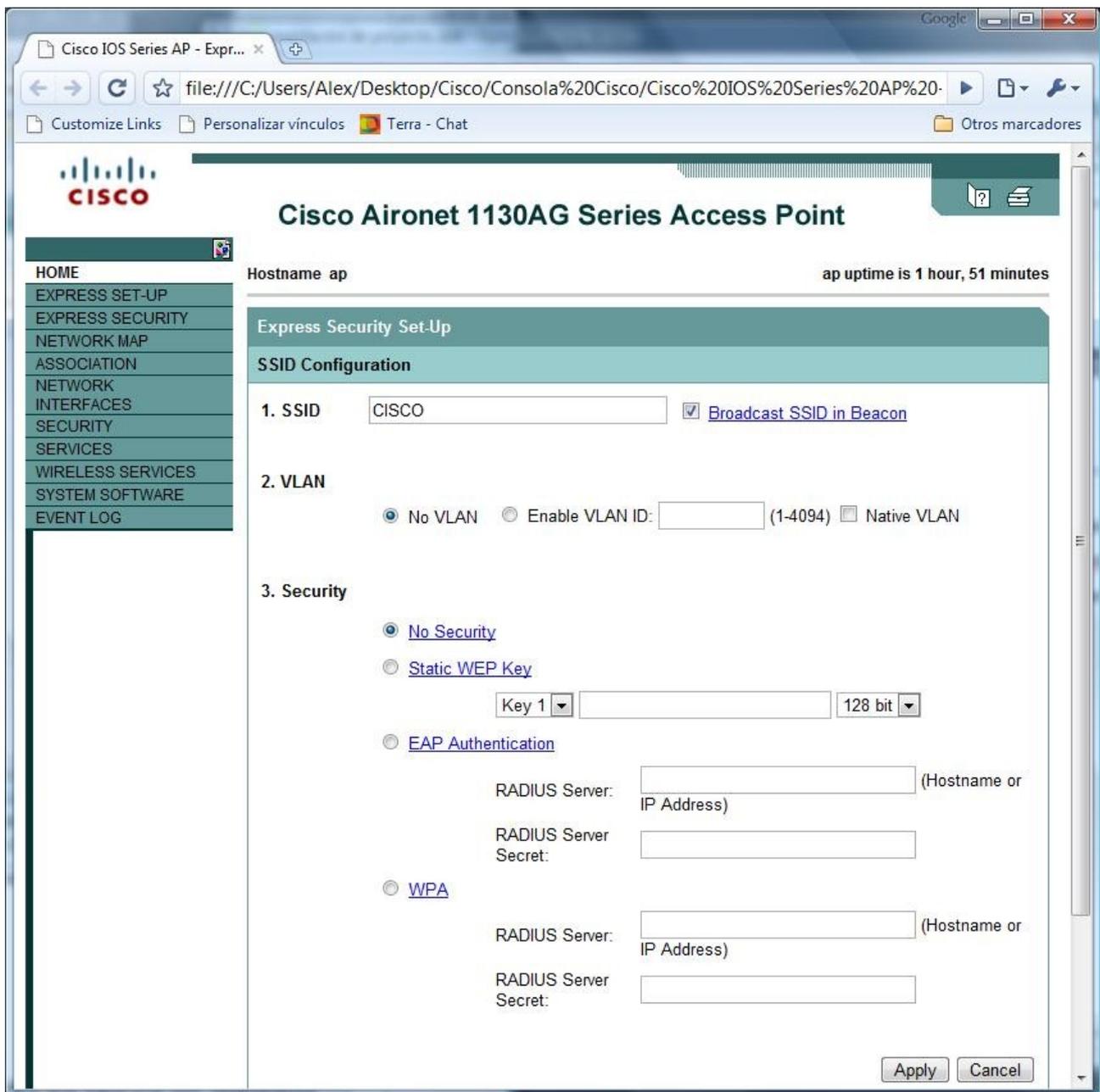
Mediante la interfaz web hay muchísimas opciones de configuración. Voy a mostrar las que hemos utilizado, que serían los apartados de SSID Manager, y de VLAN, además de la Express Security Set-Up con la que se configura todo de una forma más rápida, pero con menos opciones de configuración.

Express Security Set-Up

Desde aquí se nombra un SSID cualquiera, y se activa una VLAN cualquiera o lo dejamos sin VLAN, es decir, que el SSID muestre la red completa. En este punto trae la opción de activar el Broadcast de SSID, para que sea visto por dispositivos, en el siguiente punto veremos que esa opción no aparece.

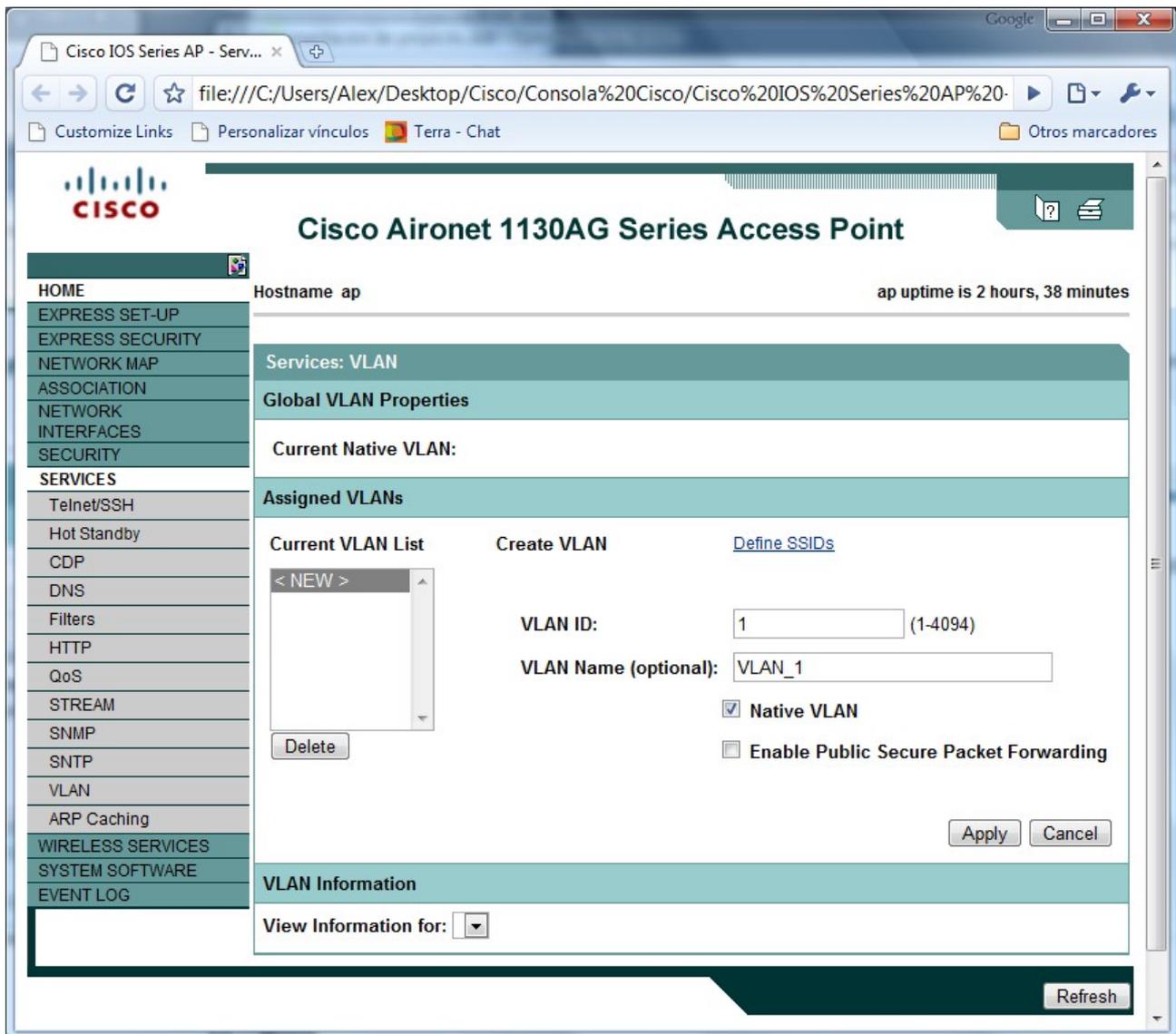
Probamos hacer un SSID de prueba, llamándolo Cisco, sin asignarle ninguna VLAN y dejándolo sin contraseña. Desde aquí sí activamos el Broadcast. El resultado mediante la interfaz web es positivo.



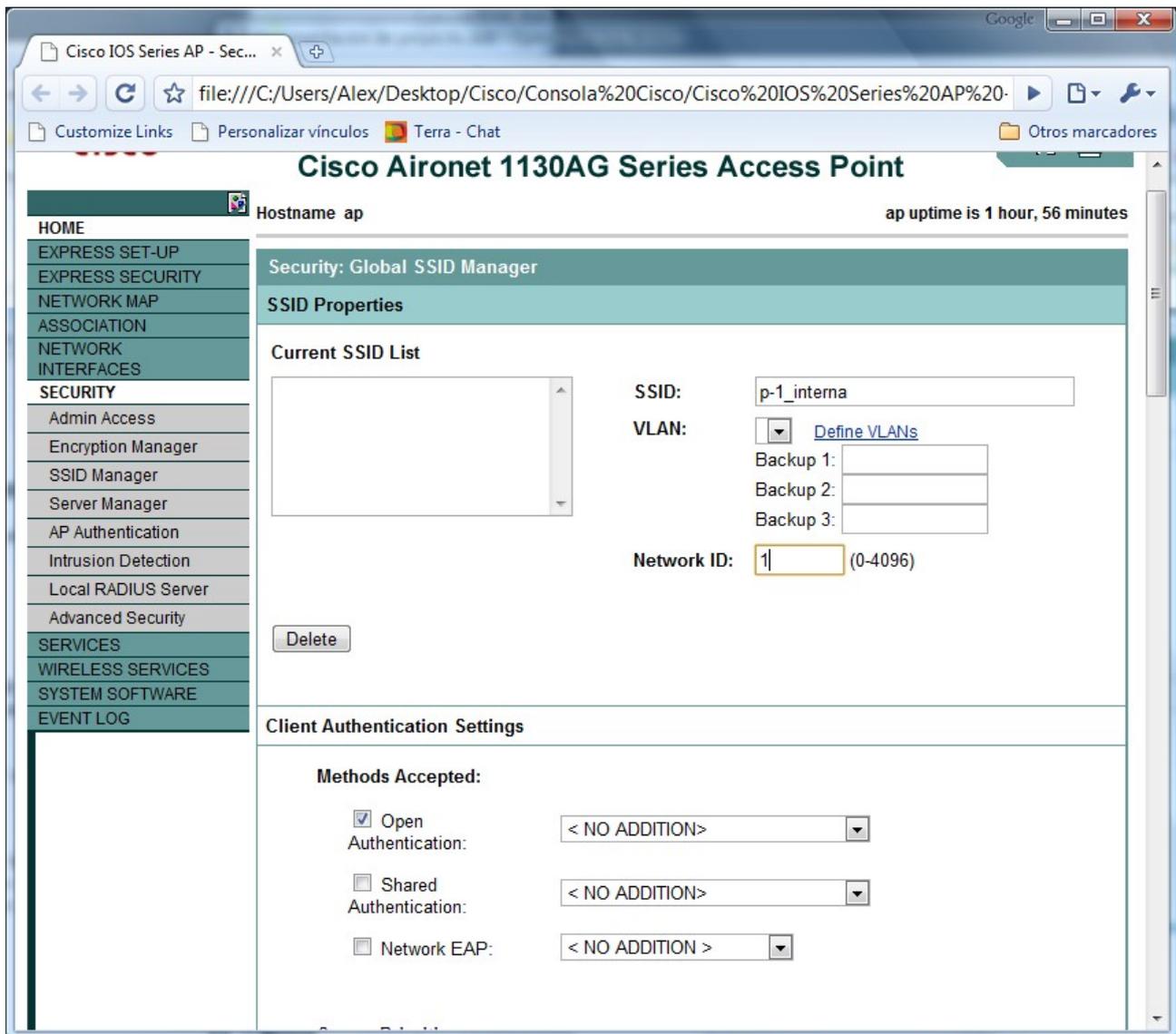


Si lo queremos hacer paso a paso, y ya asignándolo a una VLAN, nos tenemos que ir primero a activar las VLAN, dentro de la pestaña Services.

Creamos la VLAN 1, que al ser la primera, la tenemos que poner como nativa. Y una vez que le demos a aplicar, pinchamos sobre Define SSID, para irnos a la pestaña SSID Manager, dentro de Security, Podemos crear también la segunda VLAN antes de asignarla a un SSID.

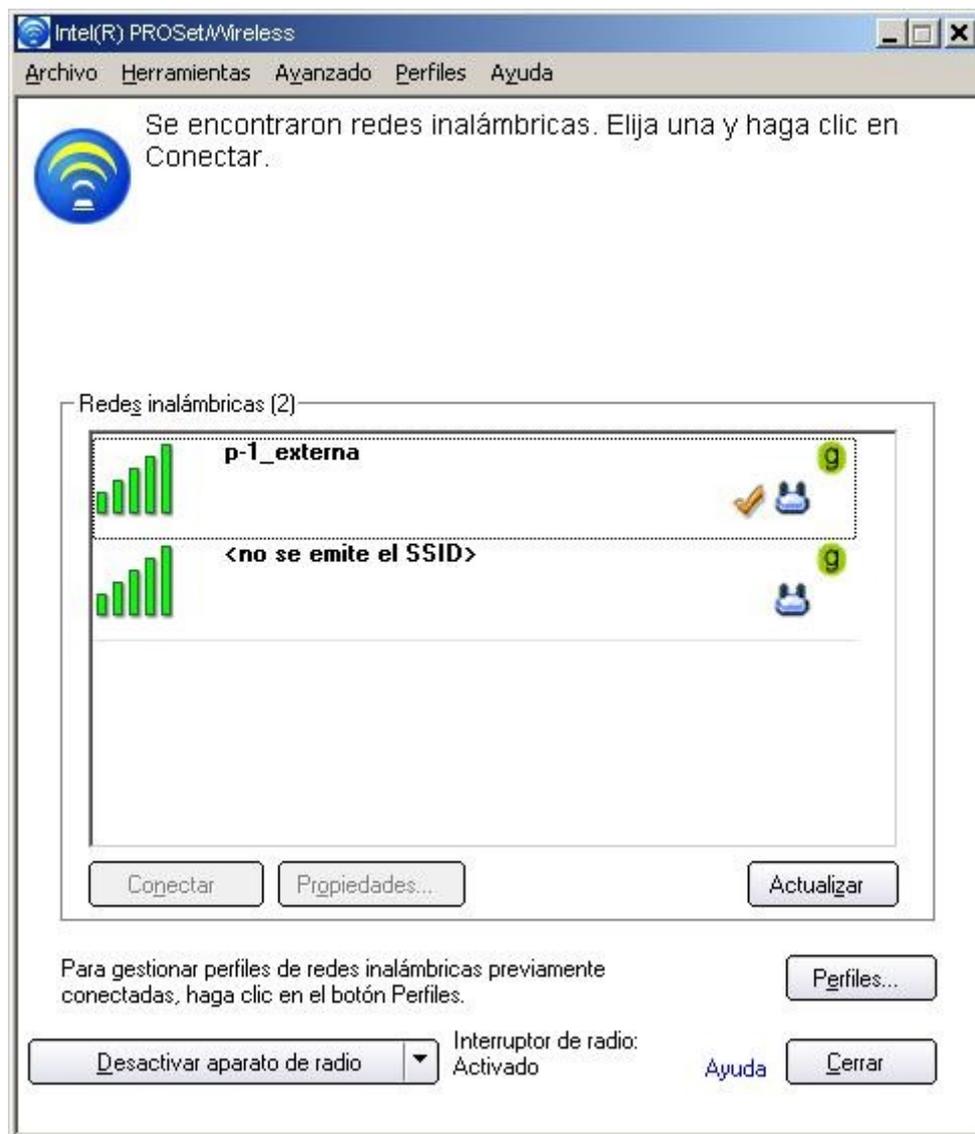


Ya aplicada, nos vamos a la página SSID Manager. Desde ahí le ponemos el nombre a las SSID, y pinchando sobre la lista de VLAN, le asignamos a cada SSID su VLAN correspondiente. En este caso, la 1, la nativa, irá para la SSID p-1_interna, es decir, para el personal interno de la empresa. Este punto es el que dió más problemas, ya que sin el Broadcast, no aparecía nada más que el SSID con la VLAN nativa.



Con este problema, indicado por los profesores, me puse en contacto con Cisco España. Desde Cisco se me dijo que tenía que tener contratado una asistencia técnica, por lo que vuelvo a llamar a otro, que amablemente me atiende hasta sus posibilidades.

Me comentó que sí que puede configurar hasta 16 SSID, pero de los cuales, solo muestra 1, dejando el resto ocultos, pero plenamente accesibles si se teclea manualmente desde cualquier pc o dispositivo móvil.



Los dos SSID daban señal al máximo, solo que uno se mostraba oculto.

No todo fue tan fácil por la interfaz web, desde un principio, era difícil que activara los radios inalámbricos a o g con los SSID, por lo que casi toda la investigación al principio fue sobre la línea de comandos. Esta fue la configuración sobre telnet para las 2 VLAN.

Creación de la primera VLAN

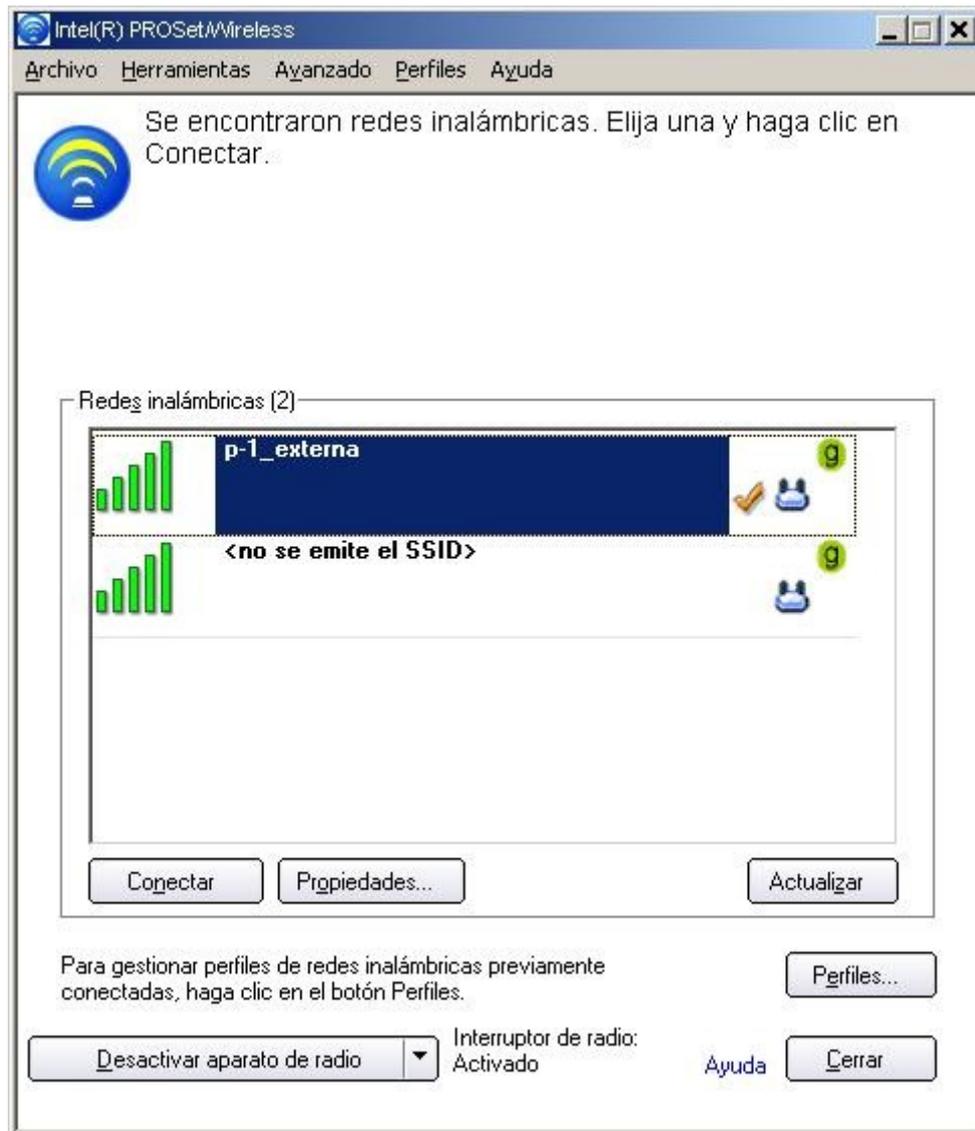
```
ap_cisco> enable
ap_cisco# configure terminal
ap_cisco(config)# interface dot11radio 0
ap_cisco(config-if)# ssid p-1_interna (SSID de la planta sótano 1, para el personal interno de la empresa)
ap_cisco(config-ssid)# vlan 1
ap_cisco(config-ssid)# exit
ap_cisco(config)# interface dot11radio 0.1
ap_cisco(config-subif)# encapsulation dot1q 1 native
ap_cisco(config-subif)# exit
ap_cisco(config)# interface fastethernet 0.1
ap_cisco(config-subif)# encapsulation dot1q 1 native
ap_cisco(config-subif)# end
```

Creación de la segunda VLAN

```
ap_cisco> enable
ap_cisco# config terminal
ap_cisco(config)# interface dot11radio 0
ap_cisco(config-subif)# ssid p-1_externa (SSID de la planta sótano 1, para el personal ajeno a la empresa)
ap_cisco(config-ssid)# vlan 2
ap_cisco(config-ssid)# exit
ap_cisco(config)# interface dot11radio 0.2
ap_cisco(config-subif)# encapsulation dot1q 2
ap_cisco(config-subif)# bridge-group 2
ap_cisco(config-subif)# exit
ap_cisco(config)# interface fastethernet 0.2
ap_cisco(config-subif)# encapsulation dot1q 2
ap_cisco(config-subif)# bridge-group 2
ap_cisco(config-subif)# end
```

9.2.- Resultados finales.

Cada vez que volvía a encender el punto de acceso cada día, siempre había algo que cada día fallaba. Pero tras la explicación de los técnicos de Cisco, con su soporte gratuito, conseguí diferenciar las 2 VLAN como se muestra en la captura.



10.- Novedades de Cisco en cuanto a puntos de acceso.

Con el objetivo de rentabilizar el uso de todo tipo de dispositivos, y de aplicaciones móviles que se dan lugar en el entorno de la empresa, en este año 2009 se ha anunciado por parte de Cisco la salida al mercado del punto de acceso **Aironet 1140**. El mes de Mayo fue el elegido para presentarlo en España, aunque desde Enero lleva siendo anunciado por la empresa. Un punto de acceso que une una fácil instalación, con todas las ventajas y prestaciones del protocolo **802.11n**. Se trata del primer producto bajo este protocolo que ofrece facilidad de uso e instalación. El primer aparato homologado basado en 802.11n, lo ofreció Cisco en el año 2007.

El Aironet 1140, incluye también el estándar **Power Over Ethernet**, con el que notarás un ahorro en mantenimiento y costes, ya que con él no será necesario alimentar independientemente el punto de acceso.

Este punto de acceso ha sido diseñado para integrar voz, video, y dispositivos móviles, lo que ayudará a incrementar el rendimiento en la empresa.

Cuenta con un diseño elegante e innovador, que favorece la reducción de gastos y la eficiencia energética. Mejora el aspecto de su predecesor, el Aironet 1130. La distribución se realizará en el llamado "paquete ecológico", que agrupa 10 puntos de acceso, que reduce el embalaje en un 50% y facilita el desembalado, la ampliación y su instalación en las organizaciones.

11.- Glosario.

Punto de acceso:

Los puntos de acceso, también llamados APs o wireless access point, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El access point o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

SSID:

El **SSID (Service Set Identifier)** es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

VLAN:

Es una forma de crear redes independientes una de otra dentro de una red física. Una red local puede ser dividida en tantas redes virtuales como queramos. Al ser virtuales, cualquier modificación que queramos hacer, no tenemos que tocar ni router, ni switch, ni cables.

Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).

En este caso, se busca crear 2 VLANs, una con la que se pueda acceder a la red local de la empresa, y otra que solo pueda acceder a internet. La primera la utilizarían los trabajadores de la empresa, y la segunda, personas externas a la empresa, que dentro del edificio, necesiten acceso a internet para cualquier cosa (exposición en reuniones, consulta de correo, etc.).

Nivel OSI de Enlace de Datos:

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del

flujo.

Nivel OSI de Red:

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan routers. En este nivel se realiza el direccionamiento lógico y la determinación la ruta de los datos hasta su receptor final.

802.11a:

Desarrollada a la misma vez que la 802.11b, y debido a su coste alto, este está dedicado a empresas, mientras que la 802.11b es la utilizada en el entorno doméstico.

La 802.11a soporta velocidades de hasta 54Mbit/s y trabaja en la frecuencia regulada de 5GHz. Comparada con la 802.11b, esta mayor frecuencia limita el rango de la 802.11a. Además, el trabajar en una frecuencia mayor significa que la señal de la 802.11a tiene una mayor dificultad para atravesar muros y objetos. Por otro lado, como la 802.11a y la 802.11b utilizan frecuencias distintas, ambas tecnologías son incompatibles entre ellas. Algunos fabricantes ofrecen híbridos 802.11a/b, aunque estos productos lo que tienen realmente son los dos extensiones implementadas.

Ventajas: Velocidad máxima alta, soporte de muchos usuarios a la vez y no produce interferencias en otros aparatos.

Inconvenientes: Alto coste, bajo rango de señal que es fácilmente obstruible.

802.11g:

Salió en 2003 para mejorar el 802.11b. Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

Ventajas: Velocidad máxima alta, soporte de muchos usuarios a la vez, rango de señal muy bueno y difícil de obstruir.

Inconvenientes: Alto coste y produce interferencias en la banda de 2.4 GHz.

802.11n:

En la actualidad la mayoría de productos son de la especificación b y de la g , sin embargo ya se ha realizado el primer borrador del estandar 802.11n que sube el límite teórico hasta los 600 Mbps. El estándar 802.11n hace uso de ambas bandas, 2,4 GHz y 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 Ghz. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

PoE:

La alimentación a través de Ethernet (**P**ower **o**ver **E**thernet, PoE) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara IP, usando el mismo cable que se utiliza para una conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Ventajas: Fuente de alimentación inteligente, es decir, se podrá apagar o reiniciar el dispositivo remotamente mediante SNMP. Los sistemas basados en PoE se pueden enchufar al SAI central, y en caso de corte de electricidad, podrá seguir funcionando sin problemas.

Desventajas: Escasa producción aún de dispositivos. Ausencia de estándares. El precio es aún bastante caro.