

## CONVERSIÓN DE ACCESS POINT DE MODO CAPWAP A MODO AUTÓNOMO Y VISCEVERSA

-  
DANIEL ORDÓÑEZ FLORES

---

### **Alcance.**

---

En el siguiente documento se mostrará el proceso para realizar la conversión de un Access Point que se encuentra operando bajo un sistema operativo de tipo CAPWAP o dependiente de un controlador a un modo de operación autónomo y visceversa. Es importante mencionar que, esta solución es diferente al modo Mobility Express, ya que tanto el proceso de conversión como las capacidades de los Access Point varían de forma importante.

### **Premisas.**

---

La siguiente sección describe las premisas y condiciones iniciales de este proceso.

- El modelo del Access Point es AIR-LAP1142N-N-K9.
- La versión del sistema operativo actual del Access Point es c1140-**k9w8**-mx.153-3.JD17.
- La alimentación eléctrica del Access Point es mediante un Power Adapter.
- Se utiliza una computadora con sistema operativo Windows 7.
- Se utiliza el software tftpd32 como servidor TFTP.
- La versión del sistema operativo autónomo será c1140-**k9w7**-tar.153-3.JD16.
- La computadora esta conectada directamente al Access Point a través de un cable RJ45.

**Notar que la versión de software *k9w8* corresponde a imágenes de Access Point que necesitan de un Wireless Lan Controller para poder ser administrado, mientras que, la versión *k9w7* corresponde a versiones de software autónomas.**

# Topología.

---

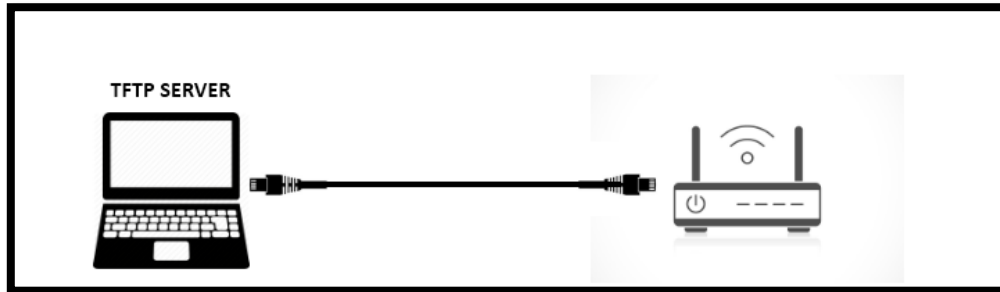


Figura 1.

# Preparativos.

---

Debido a que tenemos los equipos conectados directamente, y no hay un dispositivo que provea direccionamiento IP, será necesario realizar la asignación en forma estática, tanto en la computadora como en el Access Point. Comencemos con la computadora, para asignar el direccionamiento, nos dirigimos a nuestra tarjeta de red y configuraremos los siguientes parámetros.

- **IP:** 192.168.1.101
- **MASCARA:** 255.255.255.0

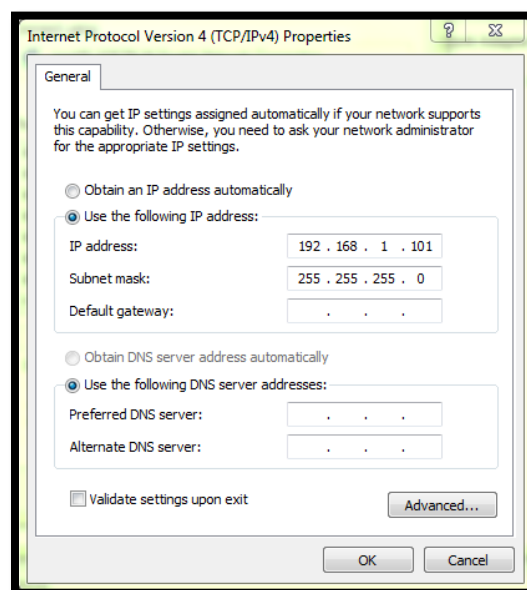


Figura 2.

Ahora, en el Access Point a través de la consola, nos solicitará credenciales para poder acceder a la interfaz de línea de comandos. Las credenciales de acceso, así como, la del modo privilegiado son “Cisco” con la letra C en mayúscula.

```
*Mar 1 03:03:58.008: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 1 03:03:59.032: %LINK-6-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 03:03:59.037: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset
*Mar 1 03:04:00.032: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
*Mar 1 03:04:00.062: %LINK-6-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 03:04:01.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to up
%Error opening flash:/capwap-saved-config (No such file or directory)
%Error opening flash:/capwap-saved-config-bak (No such file or directory)
*Mar 1 03:04:08.059: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 port 0 CLI Request Triggered
*Mar 1 03:04:09.060: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 port 514 started - CLI initiated

User Access Verification

Username: Cisco
Password:

AP70ca.9b25.45aa>enable
Password:
AP70ca.9b25.45aa#
AP70ca.9b25.45aa#
AP70ca.9b25.45aa#
```

Figura 3.

Una vez dentro del modo privilegiado, utilizaremos el comando “*debug capwap console cli*” este comando se encuentra oculto y es necesario para poder entrar en el modo de configuración del Access Point, en caso de que este comando no se utilizó y tratáramos de entrar directamente al modo de configuración, la consola nos enviaría un error en dónde nos indicaría que el comando no es aceptado o reconocido.

```
*Mar 1 03:07:58.139: %CAPWAP-3-DHCP_RENEW: Could not discover WLC. Either IP address is not assigned or assigned IP is wrong. Renewing DHCP IP.
AP70ca.9b25.45aa#
AP70ca.9b25.45aa#
AP70ca.9b25.45aa#
AP70ca.9b25.45aa#
AP70ca.9b25.45aa#conf t
^
% Invalid input detected at '^' marker.
AP70ca.9b25.45aa#
```

Figura 4.

Después de ejecutar el comando una leyenda aparecerá en dónde nos indicará que el propósito de este comando es para realizar procesos de troubleshooting y debug y que cualquier cambio puede afectar el comportamiento del equipo.

```
AP70ca.9b25.45aa#debug capwap console cli
This command is meant only for debugging/troubleshooting
Any configuration change may result in different
behavior from centralized configuration.

CAPWAP console CLI allow/disallow debugging is on
AP70ca.9b25.45aa#conf t
Enter configuration commands, one per line. End with CNTL/Z.
AP70ca.9b25.45aa(config)#
```

Figura 5.

Como se puede observar en la imagen, una vez que ingresamos el comando “*debug capwap console cli*” ya es posible acceder al contexto de configuración del equipo. Ahora, con los privilegios suficientes podremos proceder a la configuración del equipo y asignar el direccionamiento al Access Point.

La información del direccionamiento es la siguiente:

- **IP:** 192.168.1.100
- **MASCARA:** 255.255.255.0
- **DG:** 192.168.1.101

**Nota:** La asignación de direccionamiento debe de aplicarse a la interfaz Bridge Virtual Interface 1 (BVI 1)

Los comandos para realizar esta tarea son los siguientes:

```
AP70ca.9b25.45aa#configure terminal
AP70ca.9b25.45aa(config)#interface bvi 1
AP70ca.9b25.45aa(config-if)#ip address 192.168.1.100 255.255.255.0
AP70ca.9b25.45aa(config-if)#exit
AP70ca.9b25.45aa(config)#ip default-gateway 192.168.1.101
```

**Figura 6.**

Y realizmos una prueba de ping para garantizar la contividad entre el Access Point y nuestra computadora

```
AP70ca.9b25.45aa#ping 192.168.1.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
AP70ca.9b25.45aa#
```

**Figura 7.**

Por ultimo debemos de inicial nuestro servidor TFTP y seleccionar la interfaz correcta y path dónde se encuentra el archivo de nuestra imagen c1140-k9w7-tar.153-3.JD16. En nuestro ejemplo podemos observar que selecciono el adaptador de red con la dirección IP 192.168.1.101 y el path del directorio apunta a la carpeta llamada "Downloads"

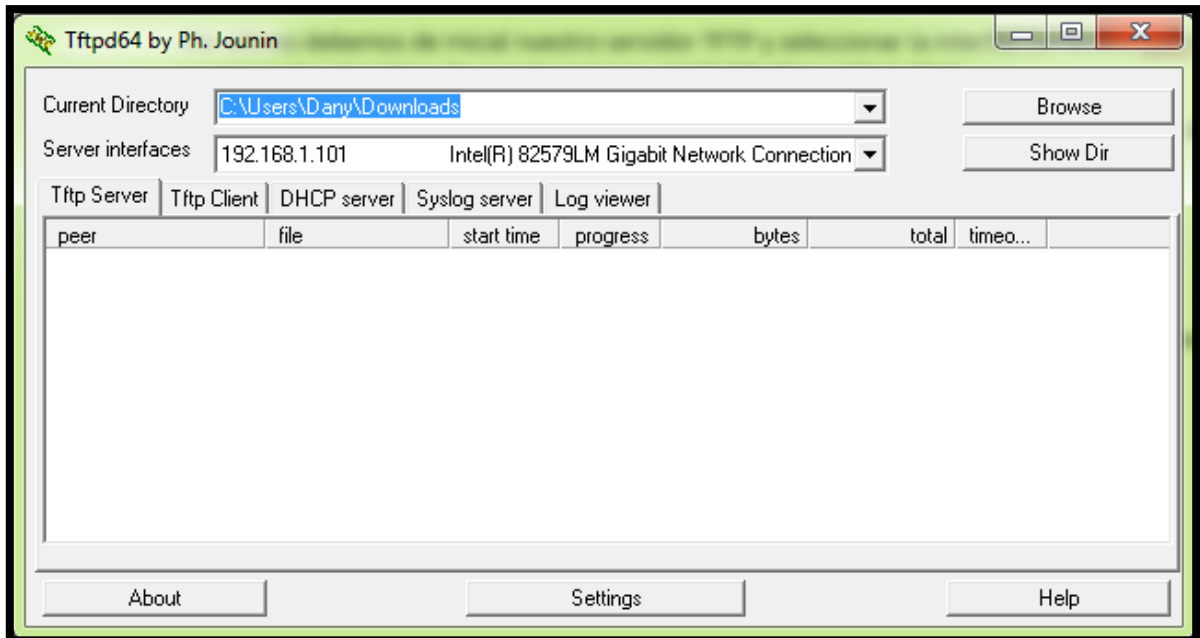


Figura 8.

# Conversión.

Por último, ejecutaremos el siguiente comando en el Access Point

**“archive download-sw /force-reload /overwrite tftp://192.168.1.101/c1140-k9w7-tar.153-3.JD16.tar”**

Una vez que la consola del AP recibe este comando, comienza con la descarga de la nueva imagen y podremos ver en el servidor TFTP el progreso del mismo.

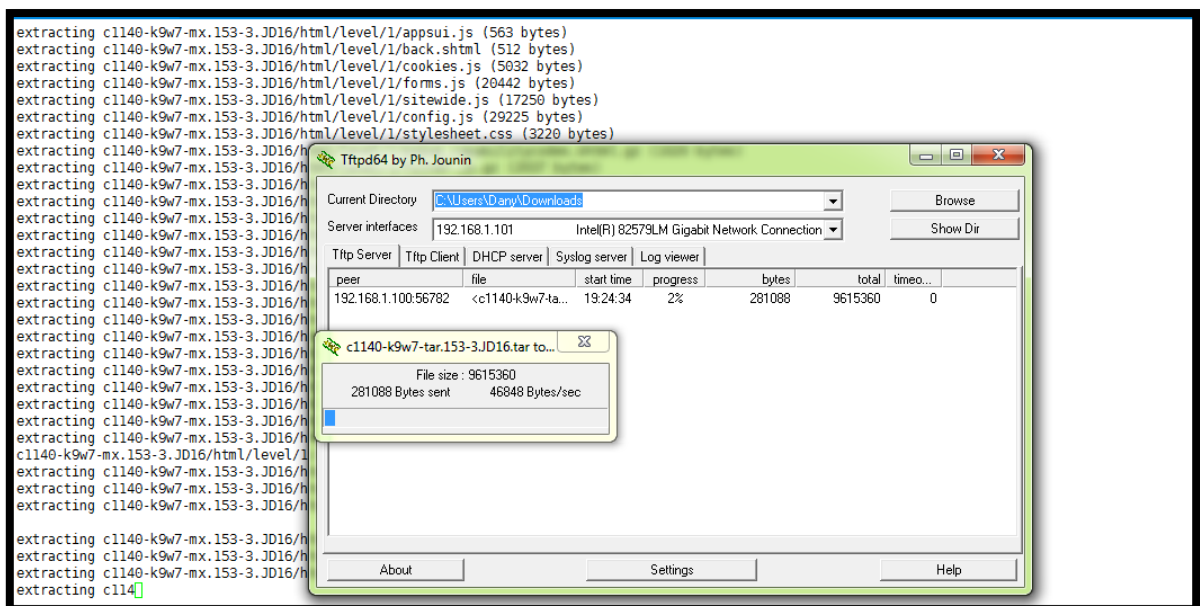


Figura 8.

# Verificación.

Cuando el Access Point termine de realizar la descarga de la nueva imagen se reiniciará y volverá a iniciar el proceso de inicio, una vez concluido se mostrará el siguiente prompt:

**ap>**

Es necesario escribir la palabra **“enable”** para entrar al modo privilegiado y será necesario introducir la palabra **“Cisco”** como contraseña.

Para verificar que el Access Point cuente con la imagen correcta será necesario ejecutar el comando “show version” y revisar que la imagen instalada ahora sea “c1140-k9w7-mx.153-3.JD16”

```
ap#show version
Cisco IOS Software, C1140 Software (C1140-K9W7-M), Version 15.3(3)JD16, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 05-Jun-18 04:10 by prod_rel_team

ROM: Bootstrap program is C1140 boot loader
BOOTLDR: C1140 Boot Loader (C1140-BOOT-M) Version 12.4(23c)JA1, RELEASE SOFTWARE (fc1)

ap uptime is 7 minutes
System returned to ROM by reload
System image file is "flash:/c1140-k9w7-mx.153-3.JD16/c1140-k9w7-xx.153-3.JD16"
Last reload reason:

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

ap#
```

Figura 9.

Para iniciar la configuración del Access Point puede realizarse a través del modo de líneas de comandos o por medio de la interfaz web. Para acceder a este ultima solo hay que ingresar la dirección IP que se contenga la interface BVI en nuestro navegador. Las credenciales al igual que en la interfaz CLI es la palabra “Cisco”.

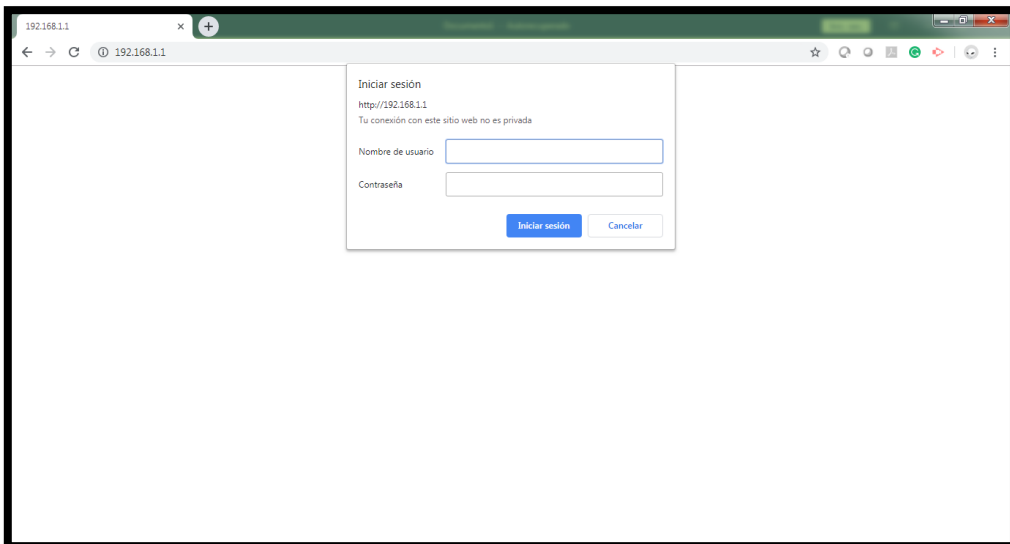


Figura 10.

Dentro del foro de Soporte de Cisco en Español se encuentra un documento llamado “Caso Práctico Access Point Autónomo” el cual puede servir de guía de configuración.

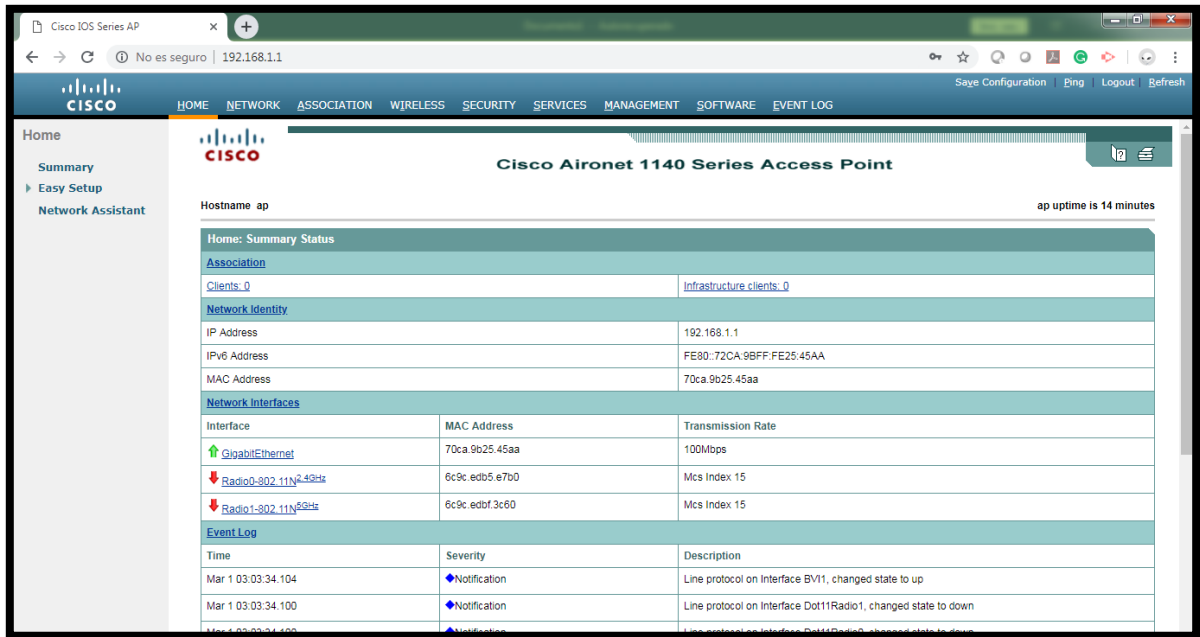


Figura 11.

## Resumen.

La siguiente sección solo muestra las líneas de comandos necesarios para realizar la conversión del Access Point, sin pantallas ni explicación detallada.

```
AP70ca.9b25.45aa#debug capwap console cli
AP70ca.9b25.45aa#configure terminal
AP70ca.9b25.45aa (config)#interface bVI 1
AP70ca.9b25.45aa (config-if)#ip address 192.168.1.100 255.255.255.0
AP70ca.9b25.45aa (config-if)#exit
AP70ca.9b25.45aa (config)#ip default-gateway 192.168.1.101
AP70ca.9b25.45aa#archive download-sw /force-reload /overwrite
tftp://192.168.1.101/c1140-k9w7-tar.153-3.JD16.tar
```