

@DanielOrdonezMX

CASO PRÁCTICO ACCESS POINT AUTÓNOMO

Creación de una WLAN Seguridad WPA2 - Daniel Ordóñez Flores

La siguiente sección indica los pasos necesarios para configurar un Access Point en forma Autónoma con seguridad local WPA2.

El primer paso para configurar el Access Point Autónomo es ingresar al portal de administración del equipo. En caso de que sea la primera vez que el AP se ha encendido por defecto la dirección ip de su portal de administración es: 10.0.0.1. La ventana de autenticación se mostrara y nos solicitará un nombre de usuario y contraseña. El campo de "Nombre" debe de quedar en blanco y en "Contraseña" deberemos escribir la palabra Cisco.

The screenshot displays the 'Express Set-Up' configuration page for a Cisco Aironet 1260 Series Access Point. The interface includes a navigation menu on the left with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, EVENT LOG, and LOGOUT. The main content area is titled 'Express Set-Up' and contains the following configuration fields:

- Host Name:** AP
- MAC Address:** 70ca.9b4b.697f
- Configuration Server Protocol:** DHCP (selected), Static IP
- IP Address:** 10.0.0.1
- IP Subnet Mask:** 255.255.255.0
- Default Gateway:** 255.255.255.255
- SNMP Community:** defaultCommunity
- SNMP Community Type:** Read-Only (selected), Read-Write

Below these fields are two radio configuration sections:

- Radio0-802.11n*40Hz:**
 - Role in Radio Network:** Access Point (selected), Repeater, Root Bridge, Non-Root Bridge, Workgroup Bridge, Universal Workgroup Bridge, Client MAC: [blank], Scanner
 - Optimize Radio Network for:** Throughput (selected), Range, Default, Custom
 - Aironet Extensions:** Enable, Disable
- Radio1-802.11n*80Hz:**
 - Role in Radio Network:** Access Point (selected), Repeater, Root Bridge, Non-Root Bridge, Workgroup Bridge, Universal Workgroup Bridge, Client MAC: [blank], Scanner
 - Optimize Radio Network for:** Throughput (selected), Range, Default, Custom
 - Aironet Extensions:** Enable, Disable

At the bottom right, there are 'Apply' and 'Cancel' buttons. The footer indicates 'Copyright (c) 1992-2010 by Cisco Systems, Inc.'

Paso 1. Click en "Express Set-up".

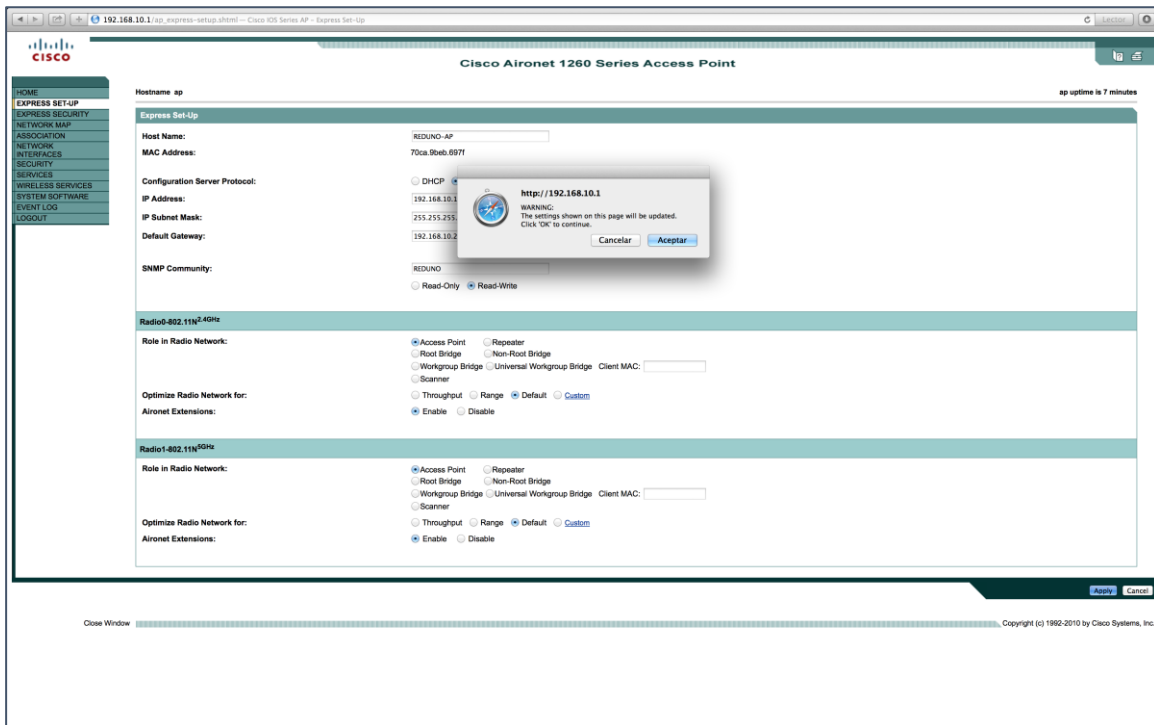
Paso 2. En el apartado "Host Name" escribir el nombre del equipo.

Paso 3. En "Configuration Server Protocol" seleccionar como el AP obtendrá su direccionamiento de administración.

Paso 4. En la sección "SNMP Community" escribir la comunidad de SNMP.

Paso 5. Click en "Read -Write" para asegurarse de que el equipo pueda ser administrado usando esta comunidad.

Paso 6. En la parte inferior de la pantalla, dar click al botón "Apply".



Paso 7. Click en “Express Set-up”.

Paso 8. Dar click en “Express Security”.

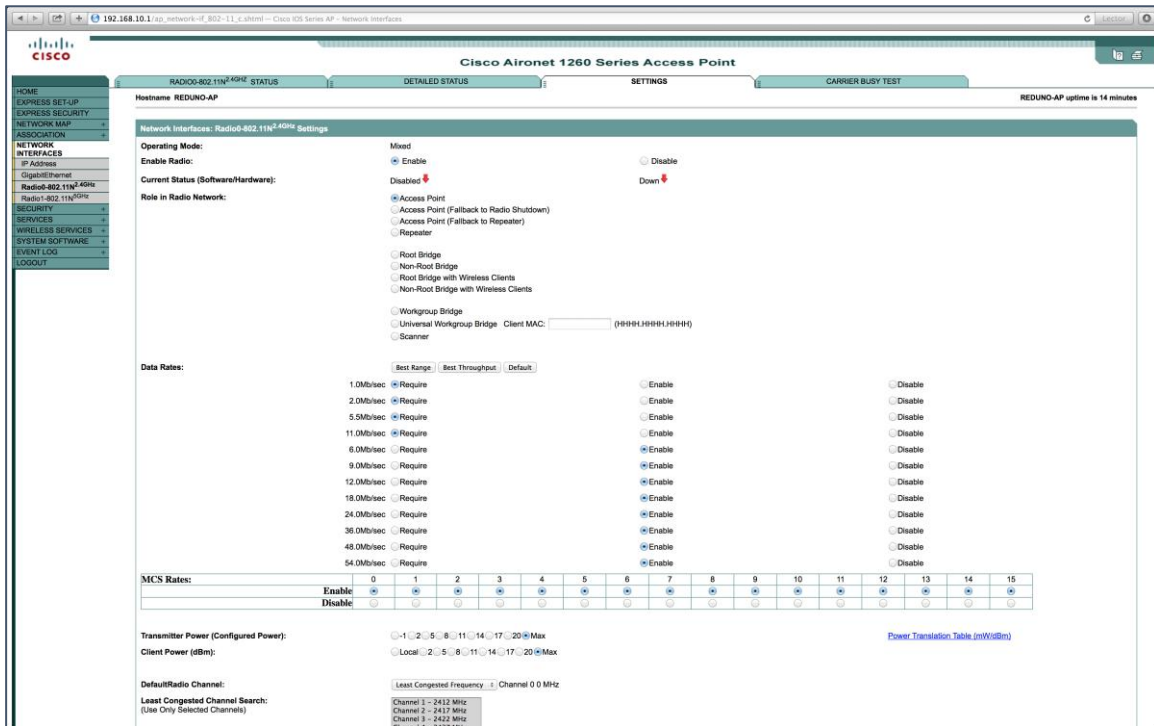
Paso 9. En el campo “SSID” escribir el nombre de la red inalámbrica.

Paso 10. Habilitar la opción “Broadcast SSID in Beacon”

Paso 11. En la sección “VLAN” escribir el numero de VLAN (SVI) donde los cliente inalámbricos tomanan sus direccionamiento.

Paso 12. En la parte inferior de la pantalla dar click al botón “Apply”.

Por defecto las interfaces inalámbricas de cualquier Access Point Autónomo se encuentran deshabilitadas administrativamente por lo cual es necesario habilitarlas.



Paso 12. Click en "Network Interfaces".

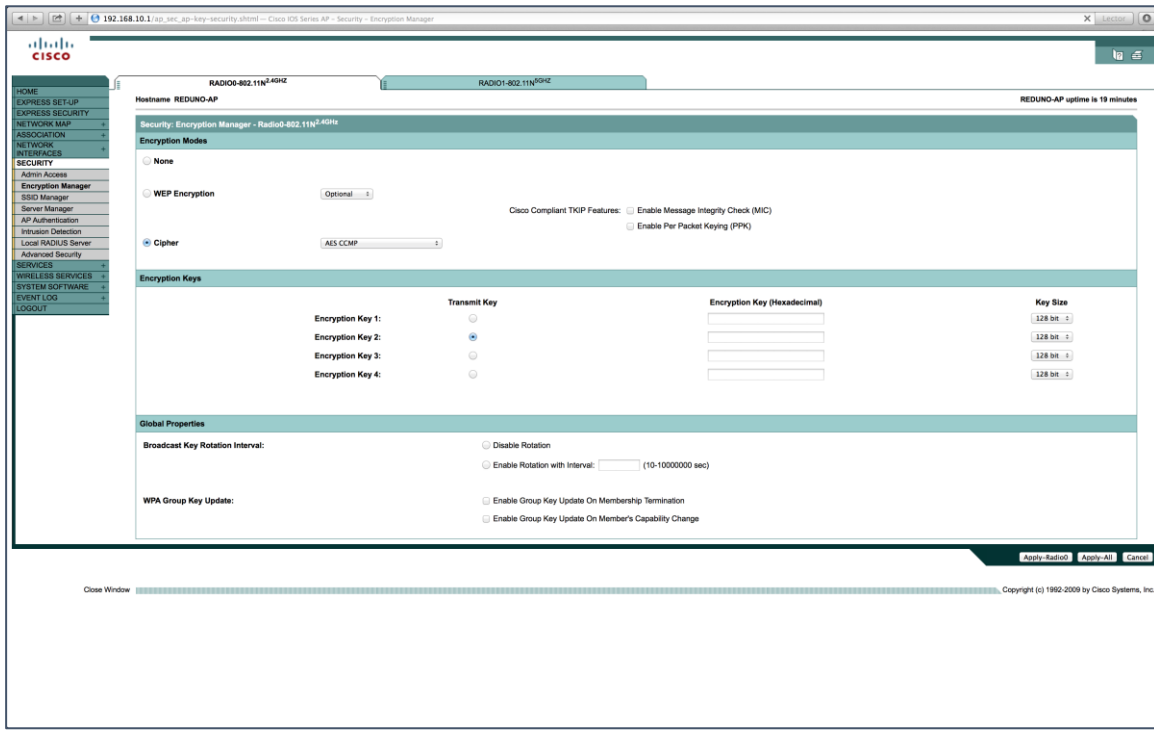
Paso 13. Click en "Radio0-802.11N 2.4Ghz".

Paso 14. Click en "Settings"

Paso 15. En la sección "Enable Radio" habilitar la opción **Enable**.

Nota Importante : Los mismos pasos se deben de realizar para el radio de 5 GHz.

Por último necesitamos configurar los parámetros de seguridad de la red inalámbrica, para lograr este objetivo debemos realizar las siguiente acciones.



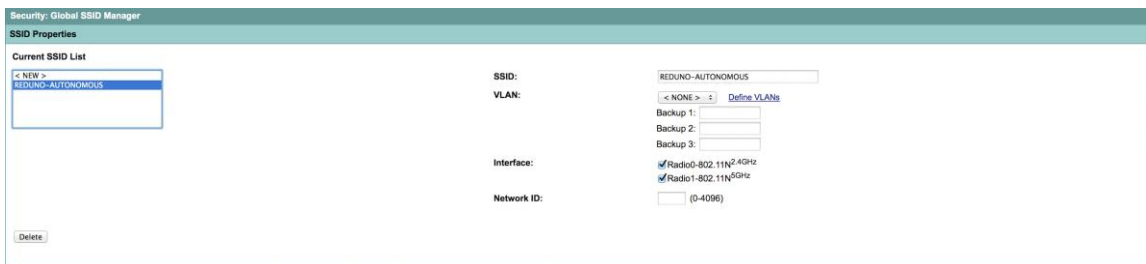
Paso 16. Click en Security y seleccionar "Encryption Manager".

Paso 17. En la sección "Encryption Modes" seleccionar "Chipers" y elegir "AES CCMP".

Paso 18. En la parte inferior de la pantalla dar click en "Apply-All".

Paso 19. Dar click en "SSID Manager".

Paso 20. Dentro de la ventana "SSID Manager" seleccionar nuestra red inalámbrica.



The screenshot shows the configuration page for Client Authenticated Key Management in the Cisco IOS Security - SSID Manager. The page is divided into several sections:

- Client Authenticated Key Management:**
 - Key Management:** A dropdown menu is set to "Mandatory". There are checkboxes for "COKM" (unchecked) and "Enable WPA" (checked). A dropdown menu for "WPAv2" is set to "WPAv2".
 - WPA Pre-shared Key:** A text field contains "*****". There are radio buttons for "ASCII" (selected) and "Hexadecimal".
- IDS Client MFP:** A checkbox "Enable Client MFP on this SSID:" is checked. A dropdown menu is set to "Optional".
- AP Authentication:** A dropdown menu for "Credentials:" is set to "< NONE >". A link "Define Credentials" is present. A dropdown menu for "Authentication Methods Profile:" is set to "< NONE >". A link "Define Authentication Methods Profiles" is present.
- Accounting Settings:**
 - Enable Accounting:** A checkbox is unchecked.
 - Accounting Server Priorities:** A radio button "Use Defaults" is selected. A link "Define Defaults" is present. A radio button "Customize" is unselected. Below are three priority dropdown menus: "Priority 1:" set to "< NONE >", "Priority 2:" set to "< NONE >", and "Priority 3:" set to "< NONE >".
- General Settings:**
 - Advertise Extended Capabilities of this SSID:** A checkbox is unchecked.
 - Advertise Wireless Provisioning Services (WPS) Support:** A checkbox is unchecked.
 - Advertise this SSID as a Secondary Broadcast SSID:** A checkbox is unchecked.
 - Enable IP Redirection on this SSID:** A checkbox is unchecked. Below it, "IP Address:" is set to "DISABLED". "IP Filter (optional):" is set to "< NONE >". A link "Define Filter" is present.
 - Association Limit (optional):** A text field contains "(1-255)".
 - EAP Client (optional):** "Username:" and "Password:" text fields are present.

Paso 21. En la sección “Client Authenticated Key Management” seleccionar **Mandatory**.

Paso 22. Elegir WPAv2.

Paso 23. Escribir la contraseña de la red inalámbrica.

VI.4. CREACIÓN DE UNA WLAN ACCESS POINT AUTÓNOMO CLI.

```
ap(config)#dot11 ssid <SSID_name>
ap(config-ssid)#vlan <vlan_id>
ap(config-ssid)#mbssid guest-mode
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa
ap(config-ssid)#wpa-psk ascii <password_SSID>
ap(config-ssid)#exit
```

¡ Creación del SSID y método de Autenticación.

```
ap(config)#int d0
ap(config-if)#encryption vlan <vlan_id> mode ciphers aes-ccm tkip
ap(config-if)#mbssid
ap(config-if)#ssid <SSID_name>
ap(config-if)#exit
```

```
i
ap(config)#int d1
ap(config-if)#enc
ap(config-if)#encryption vlan <vlan_id> mode ciphers aes-ccm tkip
ap(config-if)#mbssid
ap(config-if)#ssid <SSID_name>
ap(config-if)#exit
```

¡ Método de encriptación.

```
ap(config)#int d0. <vlan_id>
ap(config-subif)#encapsulation dot1Q <vlan_id>
ap(config-subif)#bridge-group <vlan_id>
ap(config-subif)#no shut
ap(config-subif)#exit
```

```
i
ap(config)#int d1. <vlan_id>
ap(config-subif)#encapsulation dot1Q <vlan_id>
ap(config-subif)#bridge-group <vlan_id>
ap(config-subif)#no shut
ap(config-subif)#exit
```

```
i
ap(config)#int gigabitEthernet 0. <vlan_id>
ap(config-subif)#encapsulation dot1Q <vlan_id>
ap(config-subif)#bridge-group <vlan_id>
ap(config-subif)#exit
```

```
i
ap(config)#int d0. <vlan_native>
ap(config-subif)#encapsulation dot1Q <vlan_native>native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
```

```
i
ap(config)#int d1. <vlan_native>
ap(config-subif)#encapsulation dot1Q <vlan_native>native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
```

```
ap(config)#int gigabitEthernet 0. <vlan_native>
ap(config-subif)#encapsulation dot1Q <vlan_native> native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
```

¡Creación de las subinterfaces

VII. CASOS PRÁCTICOS ACCESS POINT AUTÓNOMO.

Con el objetivo de poder entender de mejor manera la configuraciones previamente mostradas se creo un caso representando el escenario mas básico y a la vez común que se encuentra en diferentes empresas.

VII.1. CREACIÓN DE UNA WLAN CON ACCESS POINT AUTÓNOMO.

Escenario:

Consortio Red Uno desea innovar en sus tecnologías de comunicación y ha decidido incorporar un servicio de red inalámbrica a su infraestructura ya existente. Debido a que este es un primer acercamiento la empresa a decido comprar 6 Access Point's Autónomos

También el Consorcio ha decidido que el direccionamiento de la red wireless sea un direccionamiento especifico para su pronta y fácil identificación.

Consortio Red Uno ha comprado el siguiente equipo para su nueva red inalámbrica.

Equipamiento	Cantidad
Cisco 2800 Series Router	1
WS-C3750X-12S-S	4
AIR-LAP1042N-N-K9	6

PREMISAS DEL ESCENARIO:

1.- Se cuenta con dos VLANs diferentes:

REDUNO (VLAN 10): Personal que pertenece a la compañía y debe tener acceso a los recursos de la misma.

Invitados (VLAN 15): Personal que no pertenece a la compañía para quien el acceso a la red es limitado.

2.- Todo el personal de la empresa recibe su IP desde un servidor DHCP configurado sobre un enrutador Cisco 2801. El cual cuenta con los siguientes Grupos de direcciones:

POOL REDUNO: direcciones entre la 192.168.0.3 y 192.168.0.254.

POOL INVITADOS: direcciones entre la 172.16.0.3 y 172.16.0.254

Nota Importante: Se asume que ya se tiene conocimiento pleno en la configuración de VLANs, DHCP.

CONFIGURACIONES

```
ap(config)#dot11 ssid REDUNO
ap(config-ssid)#vlan 10
ap(config-ssid)#mbssid guest-mode
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii r3dun01234
ap(config-ssid)#exit
!
ap(config)#dot11 ssid INVITADOS
ap(config-ssid)#vlan 15
ap(config-ssid)#mbssid guest-mode
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii 1nvl4d0s
ap(config-ssid)#exit
!! Creacion y configuración de contraseña del SSID

ap(config)#int d0
ap(config-if)#encryption vlan 10 mode ciphers aes-ccm tkip
ap(config-if)#mbssid
ap(config-if)#ssid REDUNO
ap(config-if)#exit
i
ap(config)#int d0
ap(config-if)#encryption vlan 15 mode ciphers aes-ccm tkip
ap(config-if)#mbssid
ap(config-if)#ssid INVITADOS
ap(config-if)#exit
i
ap(config)#int d0.10
ap(config-subif)#encapsulation dot1Q 10
```



```
ap(config-subif)#bridge-group 10
ap(config-subif)#no shut
ap(config-subif)#exit
i
ap(config)#int gigabitEthernet 0.10
ap(config-subif)#encapsulation dot1Q 10
ap(config-subif)#bridge-group 10
ap(config-subif)#exit
i
ap(config)#int d0.15
ap(config-subif)#encapsulation dot1Q 15
ap(config-subif)#bridge-group 10
ap(config-subif)#no shut
ap(config-subif)#exit
i
ap(config)#int gigabitEthernet 0.15
ap(config-subif)#encapsulation dot1Q 15
ap(config-subif)#bridge-group 15
ap(config-subif)#exit
```

!! Creacion de las sub-interfaces WLAN's.

```
ap(config)#int d0.5
ap(config-subif)#encapsulation dot1Q 5 native
ap(config-subif)#bridge-group 1
ap(config-subif)#no shut
ap(config-subif)#exit
i
ap(config)#int gigabitEthernet 0.5
ap(config-subif)#encapsulation dot1Q 99 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
```

!! Configuración de VLAN de Administración/ Nativa.

En este punto, todos los usuarios que encuentren alguno de los SSID publicados y cuente con las credenciales, logrará conectarse, y el DHCP asignará una IP de acuerdo al segmento de red (VLAN- SSID) sobre el cual esté asociado el usuario.

