

CICLO FORMATIVO DE GRADO MEDIO: SISTEMAS MICROINFORMÁTICOS Y REDES  
MÓDULO: **SERVICIOS EN RED**  
UNIDAD 9: **DESPLIEGUE DE REDES INALÁMBRICAS**

**Caso práctico 1: configuración de la seguridad en redes WiFi (25%)**

### Objetivo

En esta actividad, tendremos que configurar las redes de WiFi para los tres sitios geográficos. Se utilizarán los protocolos WEP, WPA2 PSK y WPA2 RADIUS para demostrar las diferentes configuraciones de las redes WiFi y sus consideraciones de seguridad. **Healthcare at Home** se configurará mediante el protocolo WEP. **Gotham Healthcare Branch** se configurará mediante el protocolo WPA2 PSK y **Metropolis Bank HQ** utilizará el protocolo WPA2 Radius. La asignación de direcciones IP, la configuración de red y las configuraciones de servicio ya están completas en el fichero de Packet Tracer que os dejo. Se deben utilizar los routers inalámbricos y los dispositivos cliente en las diferentes regiones geográficas para configurar varias redes inalámbricas seguras. Para ello vamos a realizar las siguientes partes:

**Parte 1: Configurar el protocolo WEP para Healthcare at Home**

**Parte 2: Configurar el protocolo WPA2 PSK para Gotham Healthcare Branch**

**Parte 3: Configurar el protocolo WPA2 RADIUS para Metropolis Bank HQ**

### Consideraciones

Vamos a utilizar la siguiente tabla de direccionamiento:

Dispositivo	Dirección IP privada	Dirección IP pública	Máscara de subred	Sitio
Servidor NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ

Es necesario responder en rojo, para facilitar la labor del profesor, a continuación de la donde ponga **Respuesta**, en la siguiente línea, utilizando este mismo fichero para responder.

Habrà que mandarle al profesor los siguientes ficheros:

- Este mismo, pero con las respuestas hechas.
- El fichero de Packet Tracer que hemos utilizado para la práctica. No se nos olvide guardar los cambios al final antes de enviarlo.

### Evaluación

Se va a utilizar la siguiente tabla para calificar:

Sección de la actividad	Ubicación de la consulta	Puntos posibles	Puntos obtenidos
Parte 1: Configurar el protocolo WEP para Healthcare at Home	Paso 2	5	
Parte 3: Configurar el protocolo WPA2 RADIUS para Metropolis Bank HQ	Paso 4	5	
<b>Preguntas</b>		<b>10</b>	
<b>Puntuación de Packet Tracer</b>		<b>90</b>	
<b>Puntuación total</b>		<b>100</b>	

## Importante

Antes que nada, hay que bajarse el fichero de Packet Tracer para hacer la práctica. Lo abrimos. Minimizamos la ventana *PT Activity*, para poder trabajar. Y en la ventana *User Profile* le damos a cancel.

## Parte 1: Configure el protocolo WEP para Healthcare at Home

### Paso 1: Configure el SSID inalámbrico.

- Haga clic en el sitio **Healthcare at Home** y luego haga clic en **PC0**.
- Seleccione la ficha **Escritorio**. Haga clic en **Símbolo del sistema**. En la petición de ingreso, introduzca el comando **ipconfig**.

```
Computadora> ipconfig
```

```
Conexión FastEthernet0: (puerto predeterminado)
```

```
Dirección Link-local IPv6.....: FE80::20B:BEFF:FEB4:1262
Dirección IP.....: 10.44.3.100
Subnet Mask (máscara de subred).....: 255.255.255.0
Gateway predeterminado.....: 10.44.3.1
```

¿Cuál es la dirección IP del gateway predeterminado?

*Respuesta:*

**10.44.3.1**

- Desplácese al **navegador web** e introduzca la dirección IP del gateway predeterminado. Cuando se le solicite, ingrese **admin** como el nombre de usuario y la contraseña. Haga clic en **Aceptar**.
- El **router inalámbrico** es el gateway predeterminado de esta red. Haga clic en la ficha **Inalámbrico**.
- Cambie el **SSID** de **DefaultWIFI** a **Home**.
- Establezca el SSID Broadcast en **Enabled**.
- Haga clic en **Save Settings** (Guardar configuración).

### Paso 2: Configurar la seguridad inalámbrica.

- En el router inalámbrico, haga clic en **Wireless > Wireless Security**.
- Haga clic en el menú desplegable y establezca el Modo de seguridad en **WEP**.
- Mantenga configurada la opción de encriptación en 40/64 bits e introduzca la clave **0123456789** como Clave 1.
- Haga clic en **Save Settings** (Guardar configuración).

El protocolo WEP y la clave 0123456789 no son seguros. ¿Por qué el protocolo WEP no se recomienda para asegurar las redes inalámbricas?

*Respuesta:*

**Porque pese a ser un protocolo cifrado con contraseña, ésta tiene pocos bits de uso, lo que se traduce en contraseñas más cortas y más fáciles de averiguar.**

**Las contraseñas que se usan son estáticas, y se establecen de forma manual, por lo que no cambiarán con el tiempo y serán más sencillas de conseguir.**

**Paso 3: Conecte los clientes.**

- a. En el sitio **Healthcare at Home** haga clic en la PC portátil de **Dave**.
- b. Haga clic en la ficha **Escritorio (Desktop)** y luego haga clic en **Computadora inalámbrica (PC Wireless)**.
- c. Haga clic en la ficha **Conectar** y luego haga clic en **Actualizar**.
- d. Seleccione el nombre de red inalámbrica **Home** y haga clic en **Conectar**.
- e. Introduzca la clave **0123456789** como Clave 1 WEP y haga clic en **Conectar**.
- a. Repita los pasos **a-e** para la PC portátil de **Mary**.

**Parte 2: Configure el protocolo WPA2 PSK para Gotham Healthcare Branch**

**Paso 1: Configure el SSID inalámbrico.**

- a. Haga clic en el sitio **Gotham Healthcare Branch** y luego haga clic en **PC1** (utiliza el botón Go back one level para volver al esquema del comienzo).
- b. Seleccione la ficha **Escritorio**. Haga clic en **Símbolo del sistema**. En la petición de ingreso, introduzca el comando **ipconfig**.

Registre la dirección IP para el gateway predeterminado:

*Respuesta:*

**10.44.2.1**

- c. Desplácese al **navegador web** e introduzca la dirección IP del gateway predeterminado. Cuando se le solicite, ingrese **admin** como el nombre de usuario y la contraseña. Haga clic en **Aceptar**.
- d. Haga clic en la ficha **Inalámbrico**.
- e. Cambie el **SSID** de **DefaultWIFI** a **BranchSite**.
- f. Cambie el canal estándar a **6 – 2.437GHz**.
- g. Establezca el SSID Broadcast en **Enabled**.
- h. Haga clic en **Save Settings** (Guardar configuración).

**Paso 2: Configurar la seguridad inalámbrica.**

- a. En el router inalámbrico, haga clic en **Inalámbrico > Seguridad inalámbrica**.
- b. Haga clic en el menú desplegable y establezca el Modo de seguridad en **WPA2 Personal**.
- c. Mantenga configurada la opción de encriptación en **AES** e introduzca la contraseña **ciscosecure**.
- d. Haga clic en **Save Settings** (Guardar configuración). Haga clic en **Continuar**.

**Paso 3: Conecte los clientes.**

- a. En el sitio **Gotham Healthcare Branch** , haga clic en la computadora de **Tim**.
- b. Haga clic en la ficha **Escritorio** y luego haga clic en **Computadora inalámbrica**.
- c. Haga clic en la ficha **Conectar** y luego haga clic en **Actualizar**.
- d. Seleccione el nombre de red inalámbrica **BranchSite** y haga clic en **Conectar**.
- e. Introduzca la clave precompartida **ciscosecure** y haga clic en **Conectar**.
- f. Repita los pasos **a-e** para la computadora de **Mike**.

**Parte 3: Configure el protocolo WPA2 RADIUS para Metropolis Bank HQ**

**Paso 1: Configure el SSID inalámbrico.**

- a. Haga clic en el sitio **Metropolis Bank HQ** y luego haga clic en **Sally**.
- b. Desplácese al **navegador web** e introduzca la dirección IP del router inalámbrico (**10.44.1.251**). Cuando se le solicite, ingrese **admin** como el nombre de usuario y la contraseña. Haga clic en **Aceptar**.
- c. Haga clic en la ficha **Wireless**. Cambie el **SSID** de **DefaultWIFI** a **HQ**.
- d. Cambie el canal estándar a **11 – 2.462GHz**.
- e. Establezca el SSID Broadcast en **Enabled**.
- f. Haga clic en **Save Settings** (Guardar configuración).

**Paso 2: Configurar la seguridad inalámbrica.**

- a. En el router inalámbrico, haga clic en **Inalámbrico > Seguridad inalámbrica**.
- b. Haga clic en el menú desplegable y establezca el Modo de seguridad en **WPA2-Enterprise**.
- c. Mantenga configurada la opción de encriptación en **AES** e introduzca las siguientes credenciales del servidor RADIUS.  
  
IP DEL SERVIDOR RADIUS: **10.44.1.252**  
  
Secreto compartido: **ciscosecure**
- d. Haga clic en **Save Settings** (Guardar configuración).

**Paso 3: Configure el servidor RADIUS.**

- a. En el sitio **Metropolis Bank HQ**, haga clic en el servidor **NTP/AAA**.
- b. Haga clic en la ficha **Servicios** y luego haga clic en **AAA**.
- c. Introduzca la siguiente información en **Configuración de la red**:  
  
Nombre del cliente: **HQ**  
  
IP del cliente: **10.44.1.251**  
  
Secreta: **ciscosecure**  
  
Tipo de servidor: **Radius**

- d. Haga clic en **Agregar (Add)**.
- e. Introduzca la siguiente información en **Configuración del usuario** y haga clic en **Agregar** para agregar el nuevo nombre de usuario:

Nombre de usuario:	<b>bob</b>	Contraseña:	<b>secretninjabob</b>
Nombre de usuario:	<b>phil</b>	Contraseña:	<b>philwashere</b>

**Paso 4: Conecte los clientes.**

- a. En el sitio **Metropolis Bank HQ**, haga clic en la computadora de **Bob**.
- b. Haga clic en la ficha **Escritorio** y luego haga clic en **Computadora inalámbrica**.
- c. Haga clic en la ficha **Perfiles** y luego haga clic en **Nuevo**.
- d. Nombre el perfil **RADIUS** y haga clic en **Aceptar**.
- e. Haga clic en **Configuración avanzada**.
- f. Introduzca el nombre de red inalámbrica **HQ** y haga clic en **Siguiente**.
- g. No modifique las configuraciones de red y haga clic en **Siguiente**.
- h. Cambie el menú desplegable Seguridad inalámbrica a **WPA2-Enterprise** y haga clic en **Siguiente**.
- i. Introduzca el nombre de inicio de sesión **bob** y la contraseña **secretninjabob** y haga clic en **Siguiente**.
- j. Haga clic en **Guardar** y luego en **Conectar a la red**.
- k. La computadora de **Bob** se conectará automáticamente. (ten un poco de paciencia y si has hecho las cosas bien, se habrá conectado).
- l. Repita los pasos **a-j** para la PC portátil de **Phil** usando la información de autenticación del Paso 3e.

Al tener en cuenta una organización grande, ¿por qué el protocolo WPA2 RADIUS es más beneficioso que el protocolo WPA2 PSK?

*Respuesta:*

**Al ser una organización más grande como una empresa, necesitaremos un control más individualizado sobre cada usuario que quiera conectarse a la red para que no ocurra ningún imprevisto.**

**Para ello creamos los usuarios personalizados dentro de la propia red, y cada uno tendrá que iniciar sesión con sus propias credenciales, al contrario que con WPA2 PSK, que tienen una contraseña para la red, sin diferenciar a cada usuario.**