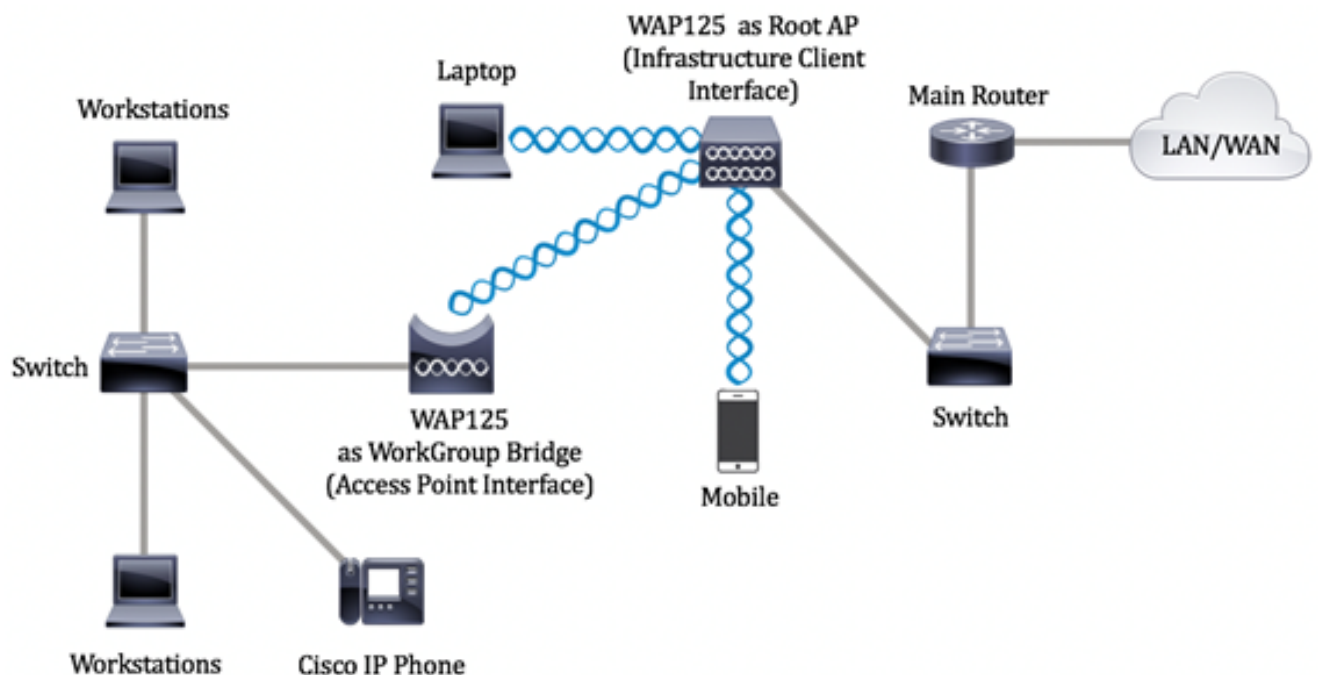


Configuración de la configuración del puente de grupo de trabajo en los puntos de acceso WAP125 o WAP581

Objetivo

La función Puente de grupo de trabajo permite al punto de acceso inalámbrico (WAP) establecer un puente entre el tráfico de un cliente remoto y la red de área local (LAN) inalámbrica conectada con el modo de puente de grupo de trabajo. El dispositivo WAP asociado con la interfaz remota se conoce como interfaz de punto de acceso, mientras que el dispositivo WAP asociado con la LAN inalámbrica se conoce como interfaz de infraestructura. El puente de grupo de trabajo permite que los dispositivos que solo tienen conexiones por cable se conecten a una red inalámbrica. Se recomienda el modo de puente de grupo de trabajo como alternativa cuando la función Wireless Distribution System (WDS) no está disponible.

La siguiente topología muestra un modelo de Workgroup Bridge. Los dispositivos con cables están vinculados a un switch, que se conecta a la interfaz LAN del WAP. En el siguiente ejemplo, el WAP125 actúa como una interfaz de punto de acceso que se conecta a la interfaz de cliente de infraestructura.



En este artículo se proporcionan instrucciones sobre cómo configurar los parámetros del puente de grupo de trabajo entre dos puntos de acceso inalámbricos.

Dispositivos aplicables

- WAP125
- WAP581

Versión del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Configuración de los parámetros del puente de grupo de trabajo

Antes de configurar el puente de grupo de trabajo en el dispositivo WAP, tenga en cuenta estas instrucciones:

- Todos los dispositivos WAP que participan en el puente de grupo de trabajo deben tener la siguiente configuración idéntica:
 - Radio
 - Modo IEEE 802.11
 - Ancho de banda del canal
 - Canal (no se recomienda Auto)

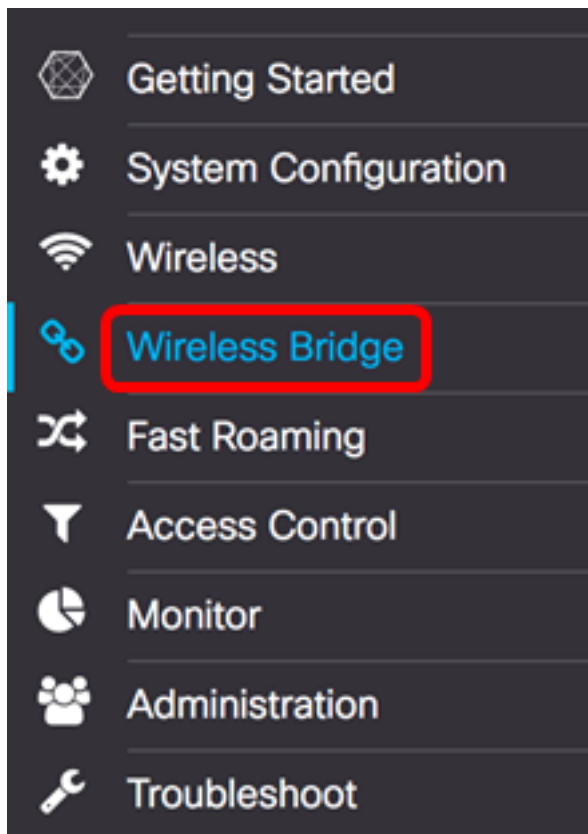
Nota: Para saber cómo configurar estos parámetros en WAP125, haga clic [aquí](#) para obtener instrucciones. Para WAP581, haga clic [aquí](#).

- Actualmente, el modo de puente de grupo de trabajo sólo admite tráfico IPv4.
- El modo de puente de grupo de trabajo no se admite en una configuración de punto único. Si tiene puntos de acceso WAP581, desactive primero SPS o agrupación en clúster antes de configurar los parámetros del puente de grupo de trabajo. Para obtener instrucciones sobre cómo configurar los parámetros SPS en su WAP, haga clic [aquí](#).

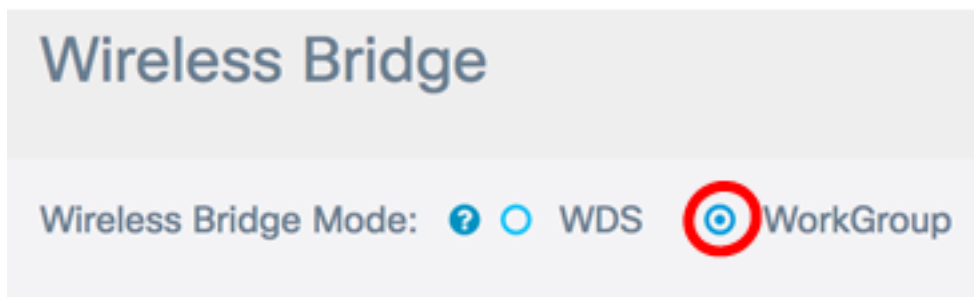
Configuración de la interfaz del cliente de infraestructura

Paso 1. Inicie sesión en la utilidad basada en web del WAP y luego elija **Wireless Bridge**.

Nota: Las opciones disponibles pueden variar en función del modelo exacto del dispositivo. En este ejemplo, se utiliza WAP125.



Paso 2. Haga clic en el botón de radio **WorkGroup**.



Paso 3. Marque la casilla de verificación **Uplink**.



<input type="checkbox"/>	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

Paso 4. Haga clic en el icono **Edit**.



<input type="checkbox"/>	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

Paso 5. Marque la casilla de verificación **Enabled** para habilitar Infrastructure Client Interface.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input checked="" type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)

Paso 6. Elija la interfaz de radio para el puente de grupo de trabajo. Cuando se configura una radio como puente de grupo de trabajo, la otra permanece operativa. Las interfaces de radio corresponden a las bandas de radiofrecuencia del WAP. El WAP está equipado para transmitir en dos interfaces de radio diferentes. La configuración de la configuración de una interfaz de radio no afectará a la otra.

Enabled	Radio
<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)
<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Nota: En este ejemplo, se elige Radio 2 (5 GHz).

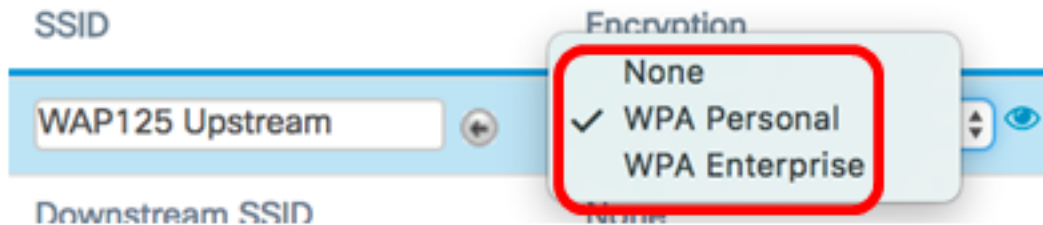
Paso 7. Introduzca el nombre del identificador del conjunto de servicios (SSID) en el campo *SSID*. Esto sirve como la conexión entre el dispositivo y el cliente remoto. Puede introducir de 2 a 32 caracteres para el SSID del cliente de infraestructura.

Nota: En este ejemplo, se utiliza WAP125 Upstream.

Radio	SSID
Radio 2 (5 GHz)	WAP125 Upstream


Nota: La flecha situada junto a SSID está disponible para el escaneo de SSID. Esta función se inhabilita de forma predeterminada y se habilita solamente si la Detección de AP está habilitada en Detección de AP rogue, que también está inhabilitada de forma predeterminada.

Paso 8. Elija el tipo de seguridad que se autenticará como estación cliente en el dispositivo WAP ascendente de la lista desplegable Cifrado. Las opciones son:



- Ninguno: seguridad abierta o no. Este es el valor predeterminado. Si selecciona esta opción, vaya directamente al [Paso 22](#).
- WPA Personal: WPA Personal admite claves de entre 8 y 63 caracteres. Se recomienda utilizar WPA2, ya que cuenta con un estándar de encriptación más eficaz.
- WPA Enterprise: WPA Enterprise es más avanzado que WPA Personal y es la seguridad recomendada para la autenticación. Utiliza protocolo de autenticación extensible protegido (PEAP) y seguridad de la capa de transporte (TLS). Vaya al [Paso 12](#) para configurar. Este tipo de seguridad se suele utilizar en un entorno de oficina y necesita un servidor RADIUS (servicio de usuario de acceso telefónico de autenticación remota) configurado. Haga clic [aquí](#) para obtener más información sobre los servidores RADIUS.

Nota: En este ejemplo, se elige WPA Personal.

Paso 9. Haga clic en el  icono y active la casilla de verificación WPA-TKIP o WPA2-AES para determinar qué tipo de encriptación WPA utilizará la interfaz cliente de infraestructura.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Nota: Si todos los equipos inalámbricos admiten WPA2, establezca la seguridad del cliente de infraestructura en WPA2-AES. El método de encriptación es RC4 para WPA y Advanced Encryption Standard (AES) para WPA2. Se recomienda utilizar WPA2, ya que cuenta con un estándar de encriptación más eficaz. En este ejemplo, se utiliza WPA2-AES.

Paso 10. (Opcional) Si ha activado WPA2-AES en el paso 9, elija una opción en la lista desplegable Management Frame Protection (MFP), tanto si desea que WAP requiera que haya tramas protegidas como si no. Para obtener más información sobre MFP, haga clic [aquí](#). Las opciones son:

- No es necesario: desactiva el soporte de cliente para MFP.
- Capaz: permite que tanto los clientes con capacidad MFP como los que no admiten MFP se unan a la red. Esta es la configuración MFP predeterminada en el WAP.
- Obligatorio: los clientes pueden asociarse sólo si se negocia MFP. Si los dispositivos no admiten MFP, no se les permite unirse a la red.

WPA Versions: WPA-TKIP WPA2-AES

MFP:

Nota: En este ejemplo, se elige Capable.

Paso 11. Introduzca la clave de encriptación WPA en el campo *Key*. La clave debe tener entre 8 y 63 caracteres. Se trata de una combinación de letras, números y caracteres especiales. Se trata de la contraseña que se utiliza al conectarse a la red inalámbrica por primera vez. Luego, vaya directamente al [Paso 21](#).

MFP:

Key: ?

Show Key as Clear Text

[Paso 12](#). Si selecciona WPA Enterprise en el paso 8, haga clic en un botón de opción del método EAP.

Las opciones disponibles se definen de la siguiente manera:

- PEAP: este protocolo proporciona a cada usuario inalámbrico bajo los nombres de usuario y contraseñas individuales WAP que soportan los estándares de encriptación AES. Dado que PEAP es un método de seguridad basado en contraseña, su seguridad Wi-Fi se basa en las credenciales del dispositivo del cliente. PEAP puede suponer un riesgo de seguridad potencialmente grave si tiene contraseñas débiles o clientes no seguros. Se basa en TLS pero evita la instalación de certificados digitales en cada cliente. En su lugar, proporciona autenticación a través de un nombre de usuario y una contraseña.
- TLS: TLS requiere que cada usuario tenga un certificado adicional para que se le conceda acceso. TLS es más seguro si dispone de los servidores adicionales y la infraestructura necesaria para autenticar a los usuarios en la red. Si elige esta opción, vaya directamente al [Paso 14](#).

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method:

 PEAP TLS

Nota: Para este ejemplo, se elige PEAP.

Paso 13. Introduzca el nombre de usuario y la contraseña del cliente de infraestructura en los campos Nombre de usuario y Contraseña. Esta es la información de inicio de sesión que se utiliza para conectarse a la interfaz de cliente de infraestructura; consulte la interfaz del

cliente de infraestructura para encontrar esta información. Luego, vaya directamente al [Paso 21](#).

EAP Method: PEAP TLS

Username:

Password:

Show Key as Clear Text

[Paso 14](#). Si hizo clic en TLS en el paso 12, introduzca la identidad y la clave privada del cliente de infraestructura en los campos Identidad y Clave privada.

EAP Method: PEAP TLS

Identity:

Private Key:

Show Key as Clear Text

Paso 15. En el área del método de transferencia, haga clic en un botón de opción de las siguientes opciones:

- TFTP: el protocolo de transferencia de archivos trivial (TFTP) es una versión simplificada y no segura del protocolo de transferencia de archivos (FTP). Se utiliza principalmente para distribuir software o autenticar dispositivos entre redes corporativas. Si hizo clic en TFTP, vaya directamente al [Paso 18](#).
- HTTP: el protocolo de transferencia de hipertexto (HTTP) proporciona un marco de autenticación simple de respuesta al desafío que puede utilizar un cliente para proporcionar un marco de autenticación.

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Nota: Si ya hay un archivo de certificado en el WAP, los campos Archivo de certificado presente y Fecha de vencimiento del certificado ya se rellenarán con la información pertinente. De lo contrario, estarán en blanco.

HTTP

Paso 16. Haga clic en el botón **Examinar** para buscar y seleccionar un archivo de certificado. El archivo debe tener la extensión de archivo de certificado adecuada (como .pem o .pfx) de lo contrario, el archivo no se aceptará.



Nota: En este ejemplo, se elige Certificate.pfx.

Paso 17. Haga clic en **Cargar** para cargar el archivo de certificado seleccionado. Saltar al [Paso 21](#).

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: Certificate.pfx

Los campos Archivo de certificado presente y Fecha de vencimiento del certificado se actualizarán automáticamente.

TFTP

[Paso 18](#). (Opcional) Si hizo clic en TFTP en el Paso 15, ingrese el nombre de archivo del archivo de certificado en el campo *Nombre de archivo*.

Transfer Method: HTTP TFTP

Filename:

Nota: En este ejemplo, se utiliza Certificate.pfx.

Paso 19. Ingrese la dirección del servidor TFTP en el campo *TFTP Server IPv4 Address*.

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Nota: En este ejemplo, 192.168.100.108 se utiliza como dirección del servidor TFTP.

Paso 20. Haga clic en el botón **Cargar** para cargar el archivo de certificado especificado.

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Los campos Archivo de certificado presente y Fecha de vencimiento del certificado se actualizarán automáticamente.

[Paso 21.](#) Haga clic en **Aceptar** para cerrar la ventana Configuración de seguridad.

El área Estado de la conexión indica si el WAP está conectado al dispositivo WAP ascendente.

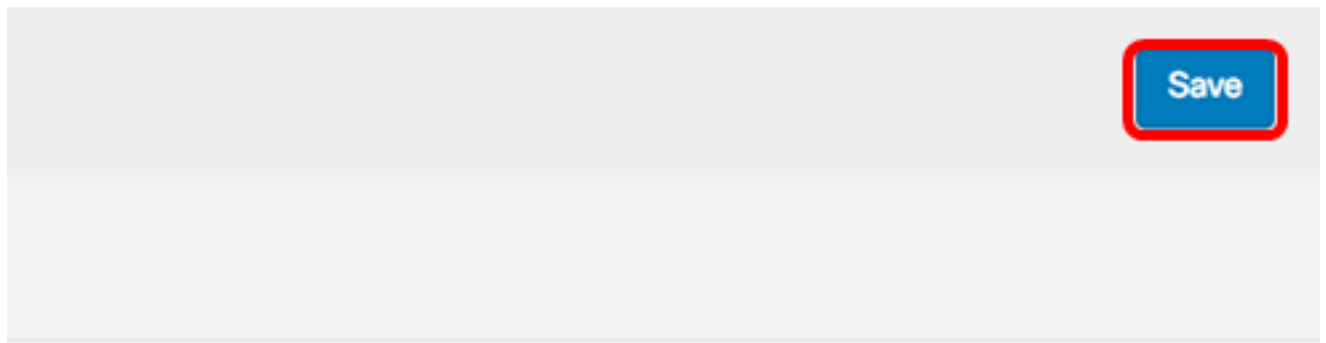
Encryption	Connection Status
<input type="text" value="WPA Personal"/> <input type="button" value="eye"/>	<input type="button" value="Disconnected"/>

[Paso 22.](#) Introduzca el ID de VLAN para la interfaz de cliente de infraestructura. El valor por defecto es 1.

Connection Status	VLAN ID
<input type="button" value="Disconnected"/>	<input type="text" value="1"/>

Nota: Para este ejemplo, se utiliza el ID de VLAN predeterminado.

Paso 23. Haga clic en **Guardar** para guardar los parámetros configurados.



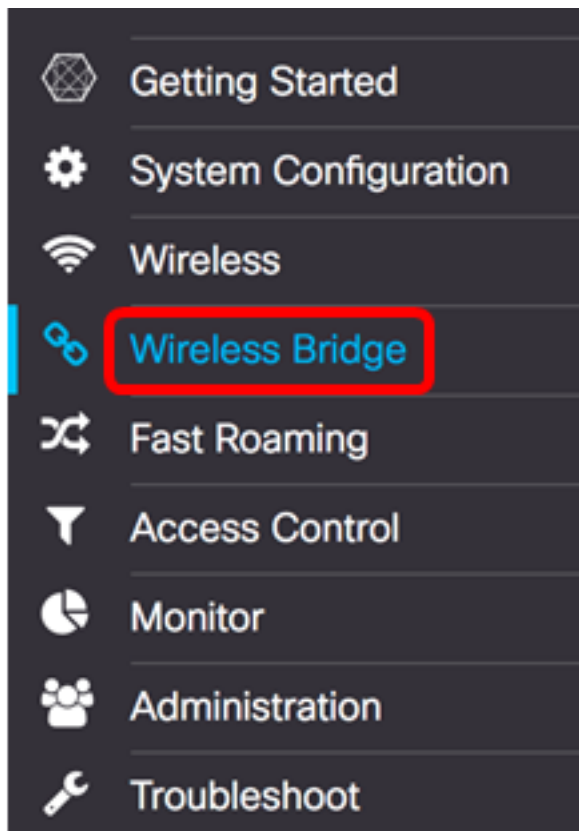
Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	<input type="text" value="1"/>	N/A	N/A
N/A	1	<input checked="" type="checkbox"/>	Disabled

Ahora debería haber configurado correctamente los parámetros de la interfaz del cliente de infraestructura en su WAP.

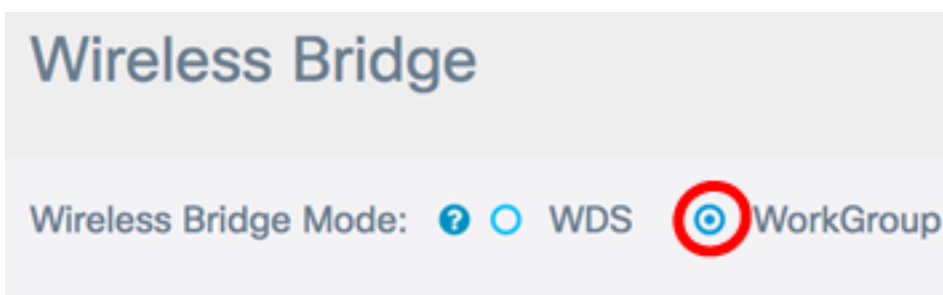
Configuración de la interfaz del cliente del punto de acceso

Paso 1. Inicie sesión en la utilidad basada en web del WAP y luego elija **Wireless Bridge**.

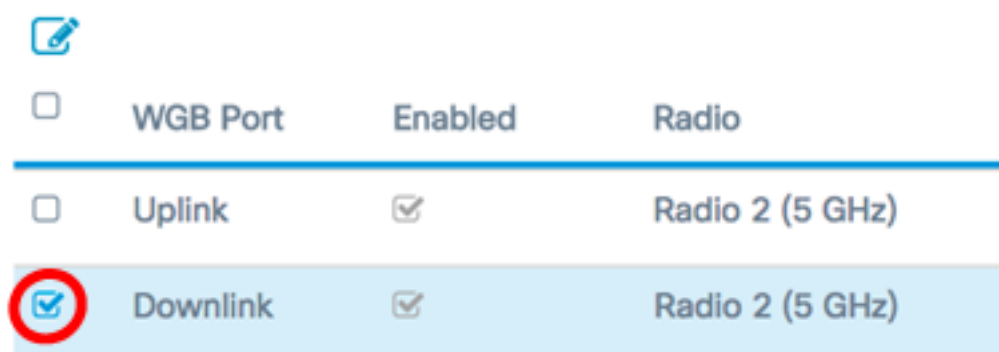
Nota: Las opciones disponibles pueden variar en función del modelo exacto del dispositivo. En este ejemplo, se utiliza WAP125.



Paso 2. Haga clic en el botón de radio **WorkGroup**.



Paso 3. Marque la casilla de verificación **Downlink**.

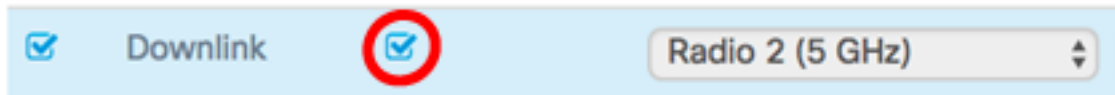


Paso 4. Haga clic en el botón **Editar**.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Paso 5. Marque la casilla de verificación **Enabled** para habilitar el bridging en la interfaz del punto de acceso.



Paso 6. Ingrese el SSID para el punto de acceso en el campo *SSID*. La longitud de SSID debe estar entre 2 y 32 caracteres. El valor predeterminado es Downstream SSID (SSID de flujo descendente).



Nota: Para este ejemplo, el SSID utilizado es WAP125 Downstream.

Paso 7. Elija el tipo de seguridad para autenticar las estaciones de cliente descendentes en el WAP de la lista desplegable Seguridad.

Las opciones disponibles se definen de la siguiente manera:

- Ninguno: abierto o sin seguridad. Este es el valor predeterminado. Vaya al [Paso 13](#) si elige esta opción.
- WPA Personal: el acceso Wi-Fi protegido (WPA) Personal admite claves de 8 a 63 caracteres. El método de encriptación es TKIP o Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP). Se recomienda utilizar WPA2 con CCMP, ya que cuenta con un estándar de encriptación avanzado (AES) más eficaz que el protocolo de integridad de clave temporal (TKIP), que utiliza sólo un estándar RC4 de 64 bits.



Paso 8. (Opcional) Marque la casilla de verificación WPA-TKIP para determinar la encriptación WPA-TKIP que utilizará la interfaz del punto de acceso. Esto se activa como opción predeterminada.

Nota: WPA-AES está atenuado y no se puede deshabilitar. En este ejemplo, WPA-TKIP está desactivado.

Security Setting

WPA Versions:

WPA-TKIP WPA2-AES

Paso 9. Introduzca la clave WPA compartida en el campo Key (Clave). La clave debe tener entre 8 y 63 caracteres y puede incluir caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales.

WPA Versions:

WPA-TKIP WPA2-AES

Key: ?

Show Key as Clear Text

Paso 10. Introduzca la velocidad en el campo Velocidad de actualización de la clave de difusión. La velocidad de actualización de la clave de difusión especifica el intervalo en el que se actualiza la clave de seguridad para los clientes asociados a este punto de acceso. La velocidad debe estar entre 0-86400, con un valor de 0 desactivando la función.

Broadcast Key Refresh Rate: ?

86400

Nota: En este ejemplo, se utiliza 86400.

Paso 11. Elija una opción de la lista desplegable MFP si desea que el WAP requiera o no tener tramas protegidas. Para obtener más información sobre MFP, haga clic [aquí](#). Las opciones son:

- No es necesario: desactiva el soporte de cliente para MFP.
- Capaz: permite que tanto los clientes con capacidad MFP como los que no admiten MFP se unan a la red. Esta es la configuración MFP predeterminada en el WAP.
- Obligatorio: los clientes pueden asociarse sólo si se negocia MFP. Si los dispositivos no admiten MFP, no se les permite unirse a la red.

Broadcast Key Refresh Rate: ?

86400

MFP:

Capable


Nota: Para este ejemplo, se elige Capable.

Paso 12. Haga clic en **Aceptar** para guardar los parámetros de seguridad.

Security Setting

WPA Versions:

WPA-TIKP WPA2-AES

Key: 

.....

Show Key as Clear Text

Broadcast Key Refresh Rate: 

86400


MFP:

Capable

OK

cancel

El área Estado de la conexión indica No aplicable o N/A.

Encryption	Connection Status
WPA Personal	Disconnected
WPA Personal 	N/A

[Paso 13.](#) Introduzca el ID de VLAN en el campo ID de VLAN para la interfaz de punto de acceso.

Nota: Para permitir el bridging de paquetes, la configuración de VLAN para la interfaz de punto de acceso y la interfaz cableada debe coincidir con la de la interfaz de cliente de infraestructura.

N/A	1	
-----	---	---

Paso 14. Marque la casilla de verificación SSID Broadcast (Difusión de SSID) si desea que se transmita el SSID descendente. SSID Broadcast (Difusión de SSID) está habilitado de forma predeterminada.

VLAN ID	SSID Broadcast	Client Filter
1	N/A	N/A

1	<input checked="" type="checkbox"/>	Disabled
---	-------------------------------------	----------

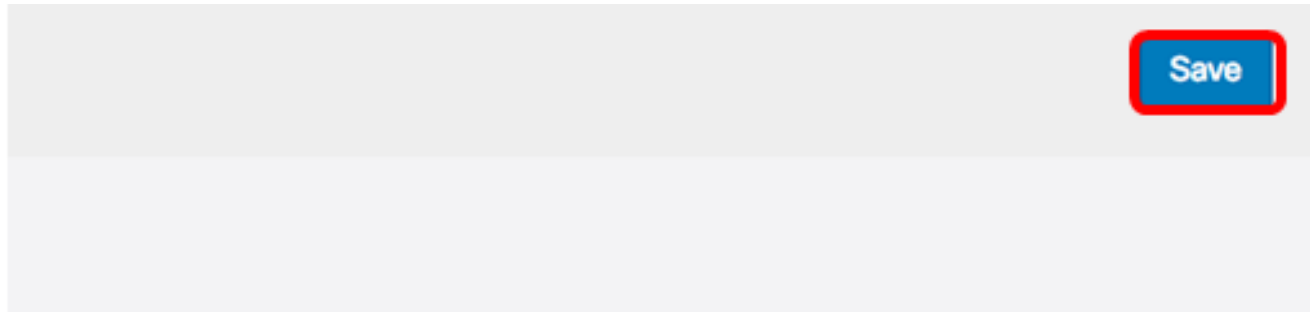
Paso 15. Elija el tipo de filtrado MAC que desea configurar para la interfaz de punto de acceso en la lista desplegable Filtrado de MAC. Cuando se habilita, se concede o se deniega a los usuarios el acceso al WAP en función de la dirección MAC del cliente que utilizan.

Las opciones disponibles se definen de la siguiente manera:

- Desactivado: todos los clientes pueden acceder a la red ascendente. Este es el valor predeterminado.
- Local: el conjunto de clientes que pueden acceder a la red ascendente está restringido a los clientes especificados en una lista de direcciones MAC definida localmente.
- RADIUS: el conjunto de clientes que pueden acceder a la red ascendente está restringido a los clientes especificados en una lista de direcciones MAC en un servidor RADIUS.

Nota: En este ejemplo, se elige Desactivado.

Paso 16. Haga clic en **Guardar** para guardar los cambios.



Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	1	N/A	N/A

N/A	1	<input checked="" type="checkbox"/>	Disabled
-----	---	-------------------------------------	----------

Ahora debería haber configurado correctamente los parámetros del puente de grupo de trabajo en los puntos de acceso inalámbricos.