

Habilitación de Varias Redes Inalámbricas en RV320 VPN Router, WAP321 Wireless-N Access Point y Switches Sx300 Series

Objetivo

En un entorno empresarial en constante cambio, la red de su pequeña empresa debe ser potente, flexible, accesible y altamente fiable, especialmente cuando el crecimiento es una prioridad. La popularidad de los dispositivos inalámbricos ha crecido exponencialmente, lo que no sorprende. Las redes inalámbricas son rentables, fáciles de implementar, flexibles, escalables y móviles, y proporcionan recursos de red sin problemas. La autenticación permite que los dispositivos de red comprueben y garanticen la legitimidad de un usuario al tiempo que protegen la red de usuarios no autorizados. Es importante implementar una infraestructura de red inalámbrica segura y manejable.

El router VPN para WAN Dual Gigabit Cisco RV320 proporciona una conectividad de acceso fiable y muy segura para usted y sus empleados. El Cisco WAP321 Wireless-N Selectable-Band Access Point con Single Point Setup admite conexiones de alta velocidad con Gigabit Ethernet. Los puentes conectan las LAN de forma inalámbrica, lo que facilita la expansión de las redes de las pequeñas empresas.

En este artículo se proporciona una guía paso a paso para la configuración necesaria para habilitar el acceso inalámbrico en una red de Cisco para pequeñas empresas, incluido el enrutamiento entre redes de área local (VLAN), varios identificadores de conjunto de servicios (SSID) y parámetros de seguridad inalámbrica en el router, el switch y los puntos de acceso.

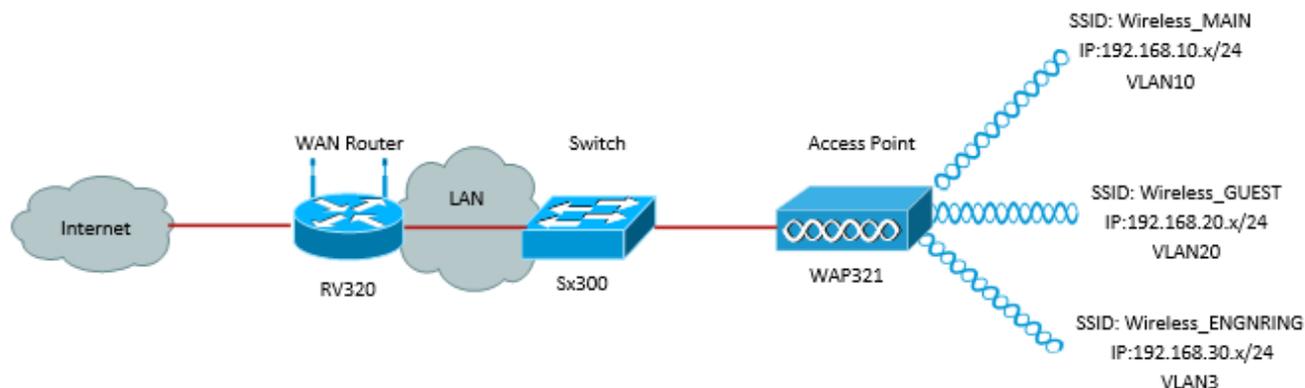
Dispositivos aplicables

Router VPN · RV320
· punto de acceso Wireless-N WAP321
Switch · Serie Sx300

Versión del software

· 1.1.0.09 (RV320)
· 1.0.4.2 (WAP321)
· 1.3.5.58 (Sx300)

Topología de red



La imagen anterior ilustra una implementación de ejemplo para el acceso inalámbrico usando varios SSID con un WAP, switch y router Cisco Small Business. El WAP se conecta al switch y utiliza la interfaz troncal para transportar varios paquetes VLAN. El switch se conecta al router WAN a través de la interfaz troncal y el router WAN realiza un ruteo entre VLAN. El router WAN se conecta a Internet. Todos los dispositivos inalámbricos se conectan al WAP.

Funciones esenciales

La combinación de la función de ruteo entre VLAN proporcionada por el router RV de Cisco con la función de aislamiento SSID inalámbrico proporcionada por un punto de acceso para pequeñas empresas proporciona una solución sencilla y segura para el acceso inalámbrico en cualquier red existente de Cisco para pequeñas empresas.

Ruteo Entre VLAN

Los dispositivos de red en diferentes VLAN no pueden comunicarse con cada uno sin un router para rutear el tráfico entre las VLAN. En una red de pequeña empresa, el router realiza el ruteo Inter-VLAN para las redes por cable e inalámbricas. Cuando se inhabilita el ruteo entre VLAN para una VLAN específica, los hosts en esa VLAN no podrán comunicarse con los hosts o dispositivos en otra VLAN.

Aislamiento SSID inalámbrico

Hay dos tipos de aislamiento SSID inalámbrico. Cuando se habilita el aislamiento inalámbrico (dentro de SSID), los hosts del mismo SSID no podrán verse entre sí. Cuando se habilita el aislamiento inalámbrico (entre SSID), el tráfico en un SSID no se reenvía a ningún otro SSID.

IEEE 802.1x

El estándar IEEE 802.1x especifica los métodos utilizados para implementar el control de acceso de redes basadas en puertos que se utiliza para proporcionar acceso de red autenticado a las redes Ethernet. La autenticación basada en puerto es un proceso que permite que solamente los intercambios de credenciales atraviesen la red hasta que el usuario conectado al puerto se autentica. El puerto se denomina puerto no controlado durante el intercambio de credenciales. El puerto se denomina puerto controlado después de completar la autenticación. Esto se basa en dos puertos virtuales existentes en un único puerto físico.

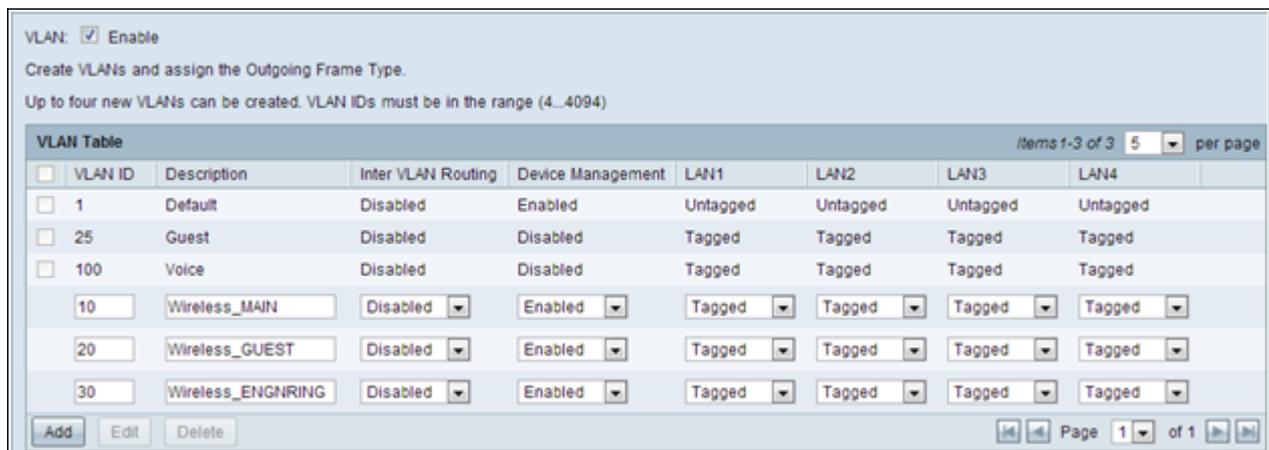
Esto utiliza las características físicas de la infraestructura LAN conmutada para autenticar

los dispositivos conectados a un puerto LAN. El acceso al puerto se puede denegar si falla el proceso de autenticación. Este estándar se diseñó originalmente para redes Ethernet por cable, pero se ha adaptado para su uso en redes LAN inalámbricas 802.11.

Configuración de RV320

En este escenario, queremos que el RV320 actúe como servidor DHCP para la red, así que necesitaremos configurarlo así como configurar VLAN separadas en el dispositivo. Para comenzar, inicie sesión en el router conectándose a uno de los puertos Ethernet y vaya a 192.168.1.1 (suponiendo que no haya cambiado la dirección IP del router).

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Administración de puertos > Afiliación VLAN**. Se abre una nueva página. Estamos creando 3 VLAN independientes para representar a diferentes audiencias objetivo. Haga clic en **Agregar** para agregar una nueva línea y editar el ID de VLAN y la Descripción. También deberá asegurarse de que la VLAN esté configurada en *Etiquetado* en cualquier interfaz en la que deban viajar.



VLAN: Enable
Create VLANs and assign the Outgoing Frame Type.
Up to four new VLANs can be created. VLAN IDs must be in the range (4..4094)

VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4
<input type="checkbox"/> 1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged
<input type="checkbox"/> 25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged
<input type="checkbox"/> 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged
<input type="text" value="10"/>	<input type="text" value="Wireless_MAIN"/>	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged
<input type="text" value="20"/>	<input type="text" value="Wireless_GUEST"/>	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged
<input type="text" value="30"/>	<input type="text" value="Wireless_ENGNRING"/>	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged

Add Edit Delete Page 1 of 1

Paso 2. Inicie sesión en la utilidad de configuración web y seleccione **Menú DHCP > DHCP Setup**. Se abre la página *DHCP Setup*:

- En el cuadro desplegable ID de VLAN, seleccione la VLAN para la que está configurando el conjunto de direcciones (en este ejemplo, VLAN 10, 20 y 30).
- Configure la dirección IP del dispositivo para esta VLAN y establezca el rango de direcciones IP. También puede activar o desactivar el proxy DNS aquí si lo desea, y esto dependerá de la red. En este ejemplo, DNS Proxy trabajará para reenviar solicitudes DNS.
- Haga clic en **Guardar** y repita este paso para cada VLAN.

DHCP Setup

IPv4 IPv6

VLAN Option 82

VLAN ID:

Device IP Address:

Subnet Mask:

DHCP Mode: Disable DHCP Server DHCP Relay

Remote DHCP Server:

Client Lease Time: min (Range: 5 - 43200, Default: 1440)

Range Start:

Range End:

DNS Server:

Static DNS 1:

Static DNS 2:

WINS Server:

TFTP Server and Configuration Filename (Option 66/150 & 67):

TFTP Server Host Name:

TFTP Server IP:

Configuration Filename:

Paso 3. En el panel de navegación, seleccione **Administración de puertos > Configuración 802.1x**. Se abre la página *Configuración 802.1X*:

- Habilite la autenticación basada en puerto y configure la dirección IP del servidor.
- RADIUS Secret es la clave de autenticación utilizada para comunicarse con el servidor.
- Elija qué puertos utilizarán esta autenticación y haga clic en **Guardar**.

802.1X Configuration

Configuration

Port-Based Authentication

RADIUS IP:

RADIUS UDP Port:

RADIUS Secret:

Port Table

Port	Administrative State	Port State
1	Force Authorized ▾	Link Down
2	Force Authorized ▾	Link Down
3	Force Authorized ▾	Link Down
4	Force Authorized ▾	Authorized

Configuración De Sx300

El switch SG300-10MP funciona como intermediario entre el router y el WAP321 para simular un entorno de red realista. La configuración en el switch es la siguiente.

Paso 1. Inicie sesión en la utilidad de configuración web y seleccione **VLAN Management > Create VLAN**. Se abre una nueva página:

Paso 2. Haga clic en Add (Agregar). Aparece una nueva ventana. Introduzca el ID de VLAN y el nombre de VLAN (utilice el mismo que la descripción de la sección I). Haga clic en Apply (Aplicar) y, a continuación, repita este paso para las VLAN 20 y 30.

VLAN

VLAN ID: (Range: 2 - 4094)

VLAN Name: (13/32 Characters Used)

Range

* VLAN Range: - (Range: 2 - 4094)

Paso 3. En el panel de navegación, seleccione **Administración de VLAN > Puerto a VLAN**. Se abre una nueva página:

- En la parte superior de la página, establezca el "ID de VLAN igual a" en la VLAN que está agregando (en este caso, VLAN 10) y luego haga clic en Ir a la derecha. Esto actualizará la página con la configuración de esa VLAN.
- Cambie la configuración en cada puerto de modo que la VLAN 10 esté ahora "Etiquetada" en lugar de "Excluida". Repita este paso para las VLAN 20 y 30.

Port to VLAN

Filter: VLAN ID equals to AND Interface Type equals to

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Access	<input type="radio"/>									
Trunk	<input checked="" type="radio"/>									
General	<input type="radio"/>									
Customer	<input type="radio"/>									
Forbidden	<input type="radio"/>									
Excluded	<input type="radio"/>									
Tagged	<input checked="" type="radio"/>									
Untagged	<input type="radio"/>									
Multicast TV VLAN	<input type="radio"/>									
PVID	<input type="checkbox"/>									

Paso 4. En el panel de navegación, seleccione **Seguridad > Radio** . Se abre la página **RADIUS**:

- Elija el método de control de acceso que utilizará el servidor RADIUS, ya sea el control de acceso de administración o la autenticación basada en puerto. Elija Port Based Access Control y haga clic en **Apply**.
- Haga clic en **Agregar** en la parte inferior de la página para agregar un nuevo servidor al que autenticarse.

RADIUS

RADIUS Accounting for Management Access can only be enabled when [TACACS+ Accounti](#)

RADIUS Accounting: Port Based Access Control (802.1X, MAC Based)
 Management Access
 Both Port Based Access Control and Management Access
 None

Paso 5. En la ventana que aparece, configurará la dirección IP del servidor, en este caso 192.168.1.32. Tendrá que establecer una prioridad para el servidor, pero dado que en este ejemplo sólo tenemos un servidor para autenticar la prioridad no importa. Esto es importante si tiene varios servidores RADIUS entre los que elegir. Configure la clave de autenticación y el resto de los parámetros se pueden dejar como predeterminados.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

✱ Server IP Address/Name:

✱ Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext)

Paso 6. En el panel de navegación, seleccione **Seguridad > 802.1X > Propiedades**. Se abre una nueva página:

- Marque **Enable** para activar la autenticación 802.1x y elija el método de autenticación. En este caso, estamos utilizando un servidor RADIUS, así que elija la primera o la segunda opción.
- Haga clic en **Apply** (Aplicar).

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID:

✱ Guest VLAN Timeout: Immediate
 User Defined

Paso 7. Elija una de las VLAN y haga clic en **Editar**. Aparece una nueva ventana. Marque **Enable** para permitir la autenticación en esa VLAN y haga clic en **Apply**. Repita el procedimiento para cada VLAN.

VLAN ID:

VLAN Name:

Authentication: Enable

Configuración de WAP321

Los puntos de acceso virtuales (VAP) segmentan la LAN inalámbrica en varios dominios de difusión que son el equivalente inalámbrico de las VLAN Ethernet. Los VAP simulan varios

puntos de acceso en un dispositivo WAP físico. El WAP121 admite hasta cuatro VAP y el WAP321 admite hasta ocho VAP.

Cada VAP se puede habilitar o inhabilitar de forma independiente, con la excepción de VAP0. VAP0 es la interfaz de radio física y permanece habilitada mientras la radio esté habilitada. Para inhabilitar el funcionamiento de VAP0, la radio misma debe ser inhabilitada.

Cada VAP se identifica mediante un identificador de conjunto de servicios (SSID) configurado por el usuario. Varios VAP no pueden tener el mismo nombre SSID. Los broadcasts SSID se pueden activar o desactivar de forma independiente en cada VAP. La difusión SSID está activada de forma predeterminada.

Paso 1. Inicie sesión en la utilidad de configuración web y seleccione **Wireless > Radio**. Se abre la página *Radio*:

- Haga clic en la casilla de verificación **Enable** para activar la radio inalámbrica.
- Click **Save**. La radio se encenderá entonces.

Radio

Global Settings

TSPEC Violation Interval: 300

Basic Settings

Radio: Enable

MAC Address: CC:EF:48:87:49:78

Mode: 802.11b/g/n

Channel Bandwidth: 20 MHz

Primary Channel: Lower

Channel: Auto

Paso 2. En el panel de navegación, seleccione **Inalámbrico > Redes**. Se abre la página *Red*:

Networks

Virtual Access Points (SSIDs)

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	Cisco1	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							
1	<input checked="" type="checkbox"/>	2	Cisco2	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							
2	<input checked="" type="checkbox"/>	3	Cisco3	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							

Add Edit Delete

Save

Nota: El SSID predeterminado para VAP0 es ciscosb. Cada VAP adicional creado tiene un nombre SSID en blanco. Los SSID para todos los VAP se pueden configurar a otros valores.

Paso 3. Cada VAP se asocia a una VLAN, que se identifica mediante un ID de VLAN (VID).

Un VID puede ser cualquier valor entre 1 y 4094, ambos inclusive. El WAP121 admite cinco VLAN activas (cuatro para WLAN más una VLAN de administración). El WAP321 admite nueve VLAN activas (ocho para WLAN más una VLAN de administración).

De forma predeterminada, el VID asignado a la utilidad de configuración para el dispositivo WAP es 1, que también es el VID sin etiqueta predeterminado. Si el VID de administración es el mismo que el VID asignado a un VAP, entonces los clientes WLAN asociados con este VAP específico pueden administrar el dispositivo WAP. Si es necesario, se puede crear una lista de control de acceso (ACL) para inhabilitar la administración de los clientes WLAN.

En esta pantalla, se deben realizar los siguientes pasos:

- Haga clic en los botones de marca de verificación del lado izquierdo para editar los SSID:
- Introduzca el valor necesario para el cuadro ID de VLAN en ID de VLAN
- Haga clic en el botón **Guardar** una vez que se hayan introducido los SSID.

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10	Wireless_MAIN	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	Show Details	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	20	Wireless_GUEST	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	Show Details	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30	Wireless_ENGNRING	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	Show Details	

Paso 4. En el panel de navegación, seleccione **Seguridad del sistema > Suplicante 802.1X**. Se abre la página *802.1X Supplicant*.

- Marque **Enable** en el campo Administrative Mode para permitir que el dispositivo actúe como suplicante en la autenticación 802.1X.
- Elija el tipo apropiado del método de protocolo de autenticación extensible (EAP) en la lista desplegable del campo Método EAP.
- Introduzca el nombre de usuario y la contraseña que utiliza el punto de acceso para obtener la autenticación del autenticador 802.1X en los campos Nombre de usuario y Contraseña. La longitud del nombre de usuario y la contraseña debe ser de 1 a 64 caracteres alfanuméricos y de símbolo. Esto ya debe configurarse en el servidor de autenticación.
- Haga clic en **Guardar para guardar la configuración**.

802.1X Supplicant

Supplicant Configuration

Administrative Mode: Enable

EAP Method: MD5

Username: example-username (Range: 1 - 64 Characters)

Password: ***** (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 18:43:36 2019 GMT

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: Choose File No file chosen

Upload

Save

Nota: El área Estado del archivo de certificado muestra si el archivo de certificado está presente o no. El certificado SSL es un certificado firmado digitalmente por una autoridad certificadora que permite al navegador web tener una comunicación segura con el servidor web. Para administrar y configurar el certificado SSL, consulte el artículo [Administración de certificados de capa de socket seguro \(SSL\) en puntos de acceso WAP121 y WAP321](#)

Paso 5. En el panel de navegación, seleccione **Security > RADIUS Server**. Se abre la página *Servidor RADIUS*. Ingrese los parámetros y haga clic en el botón **Guardar** una vez que se hayan ingresado los parámetros del servidor Radius.

RADIUS Server

Server IP Address Type: IPv4
 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)

Key-2: (Range: 1 - 64 Characters)

Key-3: (Range: 1 - 64 Characters)

Key-4: (Range: 1 - 64 Characters)

RADIUS Accounting: Enable

Save