

# Configuración de los parámetros de registro del sistema en el router serie RV34x

## Objetivo

Los eventos del sistema son actividades que pueden requerir atención y acciones necesarias para ejecutar el sistema sin problemas y evitar fallos. Estos eventos se registran como registros. Los registros del sistema permiten al administrador realizar un seguimiento de los eventos concretos que se producen en el dispositivo.

La configuración del registro define las reglas de registro y los destinos de salida para los mensajes, las notificaciones y otra información, ya que varios eventos se registran en la red. Esta función notifica al personal responsable para que se tomen las medidas necesarias cuando se produzca un evento. Los registros también se pueden enviar por correo electrónico.

En este artículo se explica cómo configurar los parámetros del registro del sistema, incluido el servidor de correo electrónico, y los parámetros del servidor remoto en el router serie RV34x.

## Dispositivos aplicables

- Serie RV34x

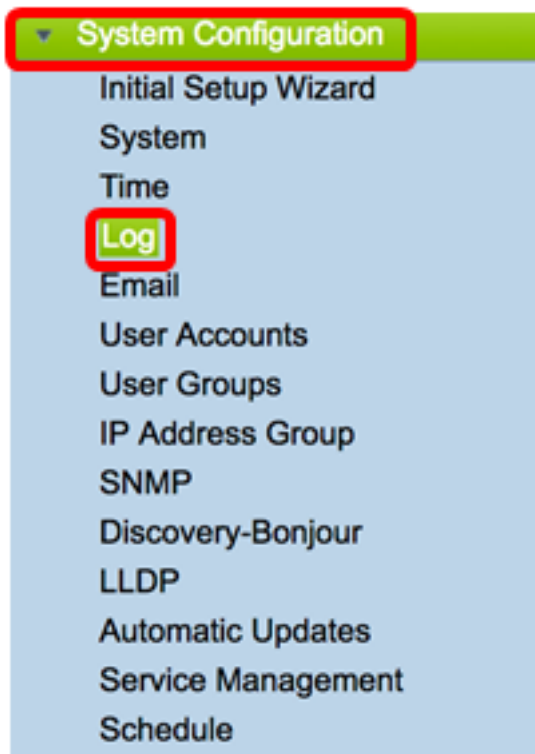
## Versión del software

- 1.0.01.14

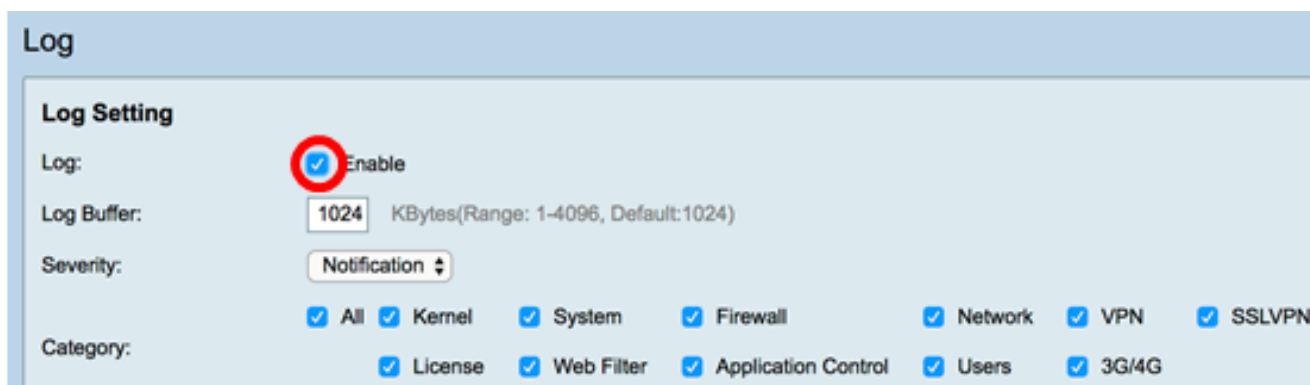
## Configuración de los parámetros de registro del sistema

### Configuración de registro

Paso 1. Inicie sesión en la utilidad basada en web y elija **Configuración del sistema > Registro**.

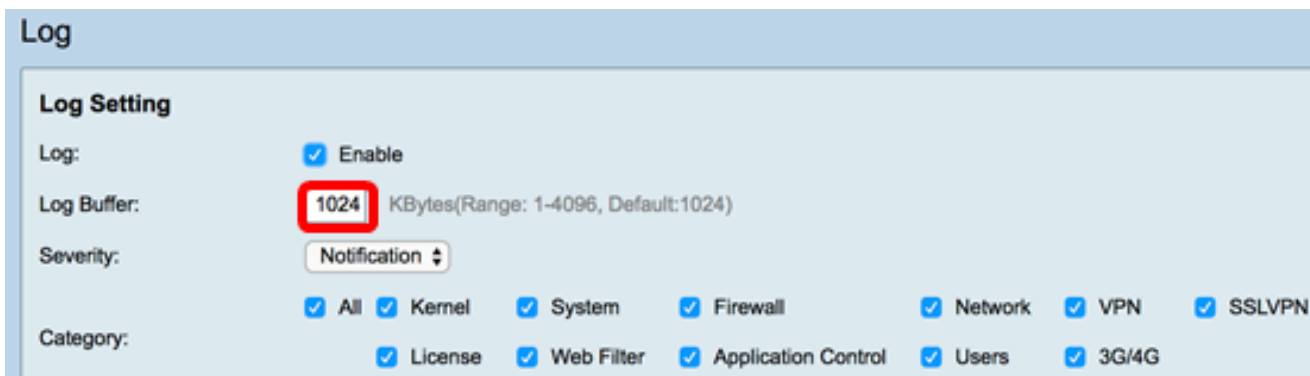


Paso 2. En el área Configuración de registro, marque la casilla de verificación **Enable** para que Log reciba actualizaciones sobre la red.



Paso 3. En el campo *Log Buffer*, introduzca el tamaño en Kilobytes (KB) que el búfer local tiene para los registros. El tamaño del búfer determina cuántos registros se pueden guardar localmente en el router. El rango va de 1 a 4096. El valor predeterminado es 1024.

**Nota:** Para este ejemplo, el valor se deja en el valor predeterminado.

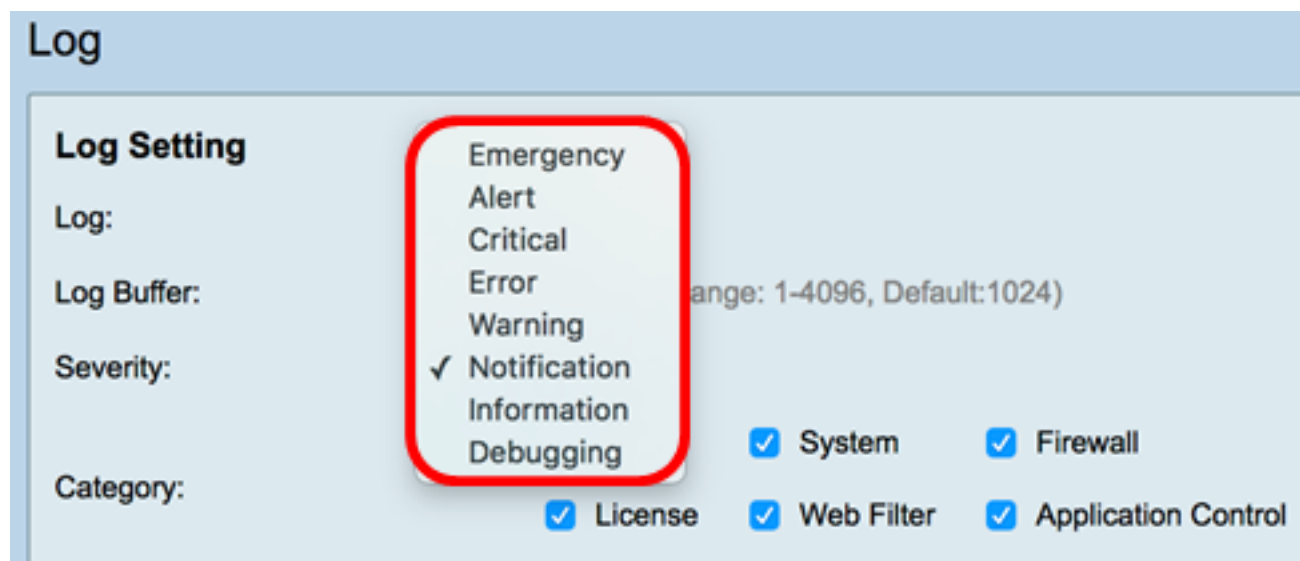


Paso 4. Elija una opción de la lista desplegable Gravedad. La gravedad elegida incluye todos los niveles superiores, por lo que los registros se mantienen para todos los niveles de gravedad desde el nivel superior hasta el nivel seleccionado.

Las opciones son:

- Emergencia - Nivel 0; El mensaje se registra si un dispositivo está inactivo o no se puede utilizar. El mensaje se transmite normalmente a todos los procesos.
- Alerta: Nivel 1; El mensaje se registra si hay un mal funcionamiento grave del dispositivo, como un caso en el que todas las funciones del dispositivo dejan de funcionar.
- Crítico — Nivel 2; El mensaje se registra si hay un mal funcionamiento crítico del dispositivo, como dos puertos que no funcionan correctamente mientras que los puertos restantes funcionan correctamente.
- Error: Nivel 3; El mensaje se registra si hay un error dentro de un dispositivo como un único puerto que está desconectado.
- Advertencia — Nivel 4; El mensaje se registra si un dispositivo funciona correctamente pero se produce un problema operativo.
- Notificación — Nivel 5; El mensaje se registra si un dispositivo funciona correctamente pero se produce un aviso del sistema. Este es el valor predeterminado.
- Información — Nivel 6; El mensaje se registra si existe una condición que no es un error en el dispositivo pero que puede requerir atención o un manejo especial.
- Depuración: nivel 7; Proporciona toda la información de depuración detallada.

**Nota:** Para este ejemplo, se elige el valor predeterminado.



Paso 5. Verifique las categorías aplicables para recibir actualizaciones y notificaciones. Las opciones son:

- All: esta opción habilita todas las opciones.
- Kernel — Registros que involucran el código del kernel.
- Sistema: registros que implican aplicaciones de espacio de usuario como el protocolo de tiempo de red (NTP), la sesión y el protocolo de configuración dinámica de host (DHCP).
- Firewall: registros activados por infracciones de firewall, reglas, ataques y filtrado de contenido.
- Red: registros relacionados con routing, DHCP, red de área extensa (WAN), red de área local (LAN) y QoS.
- VPN: registros relacionados con la red privada virtual (VPN), incluidos casos como fallo de establecimiento del túnel VPN, fallo de gateway VPN, etc.
- SSLVPN: registros relacionados con VPN de capa de conexión segura (SSL).

- Licencia: registros que implican violaciones de licencia.
- Filtro web: registros relacionados con eventos que desencadenaron el filtrado web.
- Control de aplicaciones: registros relacionados con el control de aplicaciones.
- Usuarios: registros relacionados con actividades de usuario.
- 3G/4G: registros de los dongles 3G/4G/USB conectados al router.

**Nota:** En este ejemplo, se elige Todos.

**Log Setting**

Log:  Enable

Log Buffer:  KBytes(Range: 1-4096, Default:1024)

Severity:

Category:  All  Kernel  System  Firewall  Network  VPN  SSLVPN  
 License  Web Filter  Application Control  Users  3G/4G

Save to USB Automatically:  Enable  USB1  USB2

Paso 6. (Opcional) Marque la casilla de verificación **Enable** para Guardar en USB automáticamente para guardar registros en un USB. Esto está desactivado de forma predeterminada.

**Nota:** Si el router detecta que un USB no está conectado para que esta función funcione, aparecerá una línea de texto rojo junto al botón de radio USB2 que indica que no hay USB de almacenamiento conectado y los registros se guardarán sólo después de conectar un dispositivo de almacenamiento válido.

**Log Setting**

Log:  Enable

Log Buffer:  KBytes(Range: 1-4096, Default:1024)

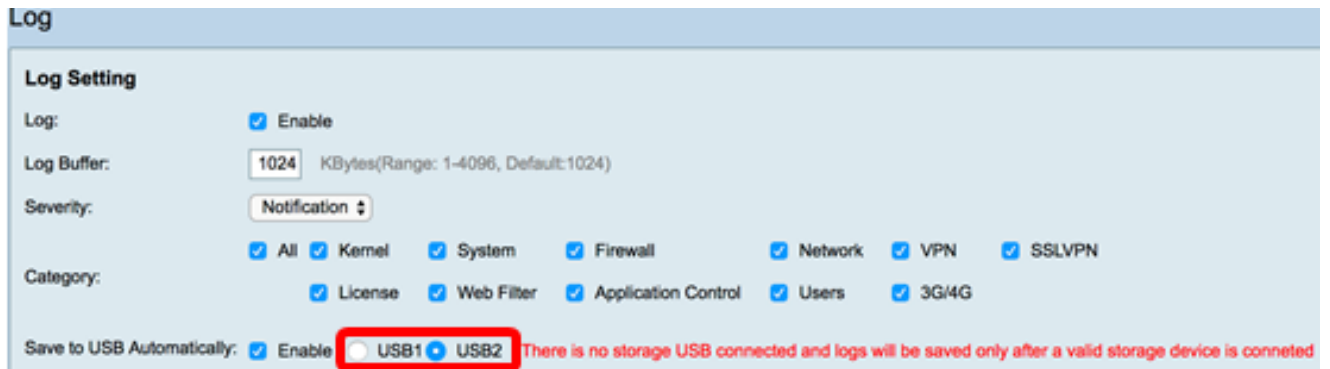
Severity:

Category:  All  Kernel  System  Firewall  Network  
 License  Web Filter  Application Control  Users

Save to USB Automatically:  Enable  USB1  USB2 There is no storage USB connected and logs w

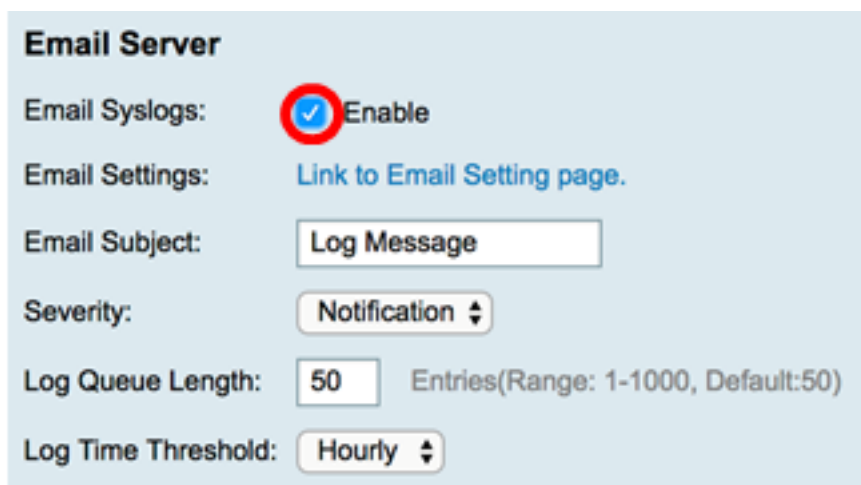
Paso 7. Elija un botón de opción del puerto USB donde está conectada la unidad.

**Nota:** Para este ejemplo, se elige USB2.

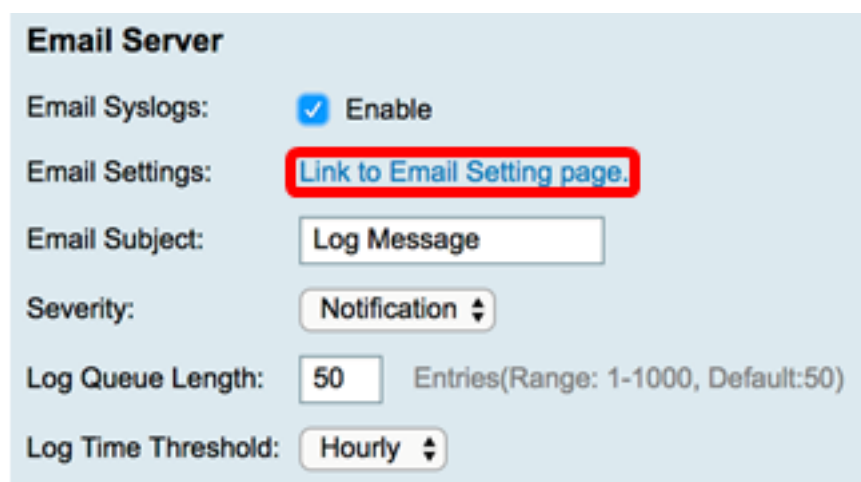


## Servidor de correo electrónico

Paso 8. Marque la casilla de verificación **Enable** para Email Syslogs para permitir que el router envíe alertas por correo electrónico para eventos o comportamientos de red específicos que puedan afectar al rendimiento, la seguridad o para fines de depuración.



Paso 9. Para configurar los parámetros de correo electrónico, haga clic en la página Enlazar a configuración de correo electrónico y haga clic [aquí](#) para obtener instrucciones sobre cómo configurar los parámetros de correo electrónico en el router serie RV34x.



Paso 10. En el campo *Asunto del correo electrónico*, introduzca un asunto para que el correo electrónico se envíe a la dirección de correo electrónico.

**Nota:** Para este ejemplo, se utiliza el mensaje de registro.

**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

Log Queue Length:  Entries(Range: 1-1000, Default:50)

Log Time Threshold:

Paso 11. En la lista desplegable Gravedad, elija una gravedad. La gravedad elegida incluye todos los niveles superiores, por lo que los registros se mantienen para todos los niveles de gravedad desde el nivel superior hasta el nivel seleccionado. Las opciones son Notificación, Advertencia, Error, Crítico, Alerta y Emergencia.

**Nota:** Para este ejemplo, se utiliza la Notificación.

**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

Log Queue Length:  Entries(Range: 1-1000, Default:50)

Log Time Threshold:

Paso 12. En el campo *Longitud de cola de registro*, ingrese el número de entradas que se deben realizar antes de que el registro se envíe al destinatario del correo electrónico. El valor predeterminado es 50.

**Nota:** Para este ejemplo, se utiliza el valor predeterminado.

**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

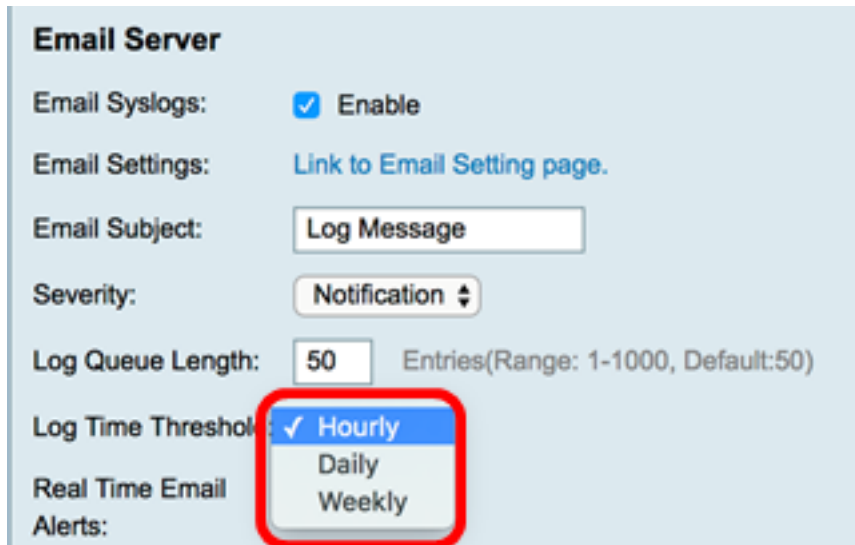
Log Queue Length:  Entries(Range: 1-1000, Default:50)

Log Time Threshold:

Paso 13. En la lista desplegable Umbral de tiempo de registro, elija el intervalo en el que el

router envía el registro al correo electrónico. Las opciones son Hourly, Daily y Weekly.

**Nota:** Para este ejemplo, se elige Hora.



**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

Log Queue Length:  Entries(Range: 1-1000, Default:50)

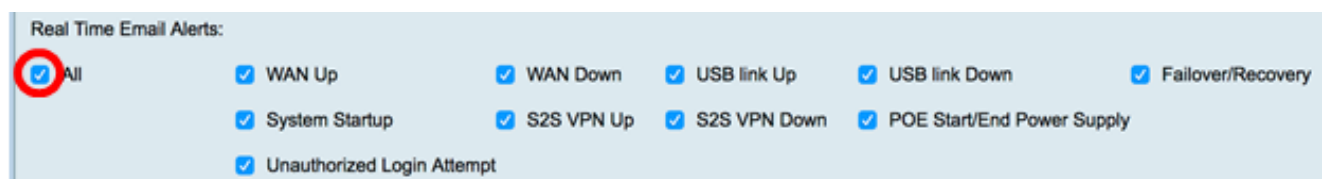
Log Time Threshold:  Hourly  
 Daily  
 Weekly

Real Time Email Alerts:

Paso 14. Active las casillas de verificación de los eventos que activarán una alerta de correo electrónico en tiempo real. Las opciones son las siguientes:

- Todos: marca todas las casillas de verificación y permite al router enviar alertas en tiempo real al correo electrónico.
- WAN Up: alerta enviada al correo electrónico sobre el enlace WAN activado.
- WAN Apagado: alerta enviada al correo electrónico sobre el enlace WAN que se ha caído.
- Enlace USB activo: alerta enviada al correo electrónico sobre el enlace USB que se está activando.
- Enlace USB inactivo: alerta enviada al correo electrónico sobre el enlace USB que se está apagando.
- Conmutación por fallo/recuperación: alerta enviada al correo electrónico sobre el router que entra en modo de recuperación o el router ha recurrido al dispositivo de seguridad USB 3G/4G para conectarse a Internet.
- Inicio del sistema: alerta enviada al correo electrónico sobre el inicio del router.
- S2S VPN Down: alerta enviada al correo electrónico de que la VPN de sitio a sitio está activa.
- S2S VPN Down: alerta enviada al correo electrónico de que la VPN de sitio a sitio está inactiva.
- Intento de inicio de sesión no autorizado: se envía una alerta al correo electrónico sobre un intento de inicio de sesión no autorizado en el router.

**Nota:** Para este ejemplo, Todos está activado.



Real Time Email Alerts:

All  WAN Up  WAN Down  USB link Up  USB link Down  Failover/Recovery

System Startup  S2S VPN Up  S2S VPN Down  POE Start/End Power Supply

Unauthorized Login Attempt

## Servidores Syslog Remotos

Paso 15. Marque la casilla de verificación **Enable** para Syslog Servers.



**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Paso 16. En el campo *Syslog Server 1*, introduzca la dirección IP del mando a distancia syslog servidor donde se almacenarán los eventos registrados.

**Nota:** Para este ejemplo, 192.168.1.102 se utiliza como remoto syslog dirección del servidor.

**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Paso 17. (Opcional) En el campo *Syslog Server 2*, ingrese la dirección IP de respaldo del mando a distancia syslog servidor.

**Nota:** En este ejemplo, se utiliza 192.168.1.109.

**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Paso 18. Haga clic en Apply (Aplicar).




**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Paso 19. (Opcional) Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en  icono en la parte superior de la página.

Ahora debería haber configurado correctamente los parámetros de registro del sistema en el router serie RV34x.