Ruteo Inter-VLAN en un Router RV34x con Restricciones de ACL Dirigidas

Objetivo

En este artículo se explica cómo configurar el routing de red de área local (VLAN) entre redes en un router serie RV34x con lista de control de acceso (ACL) dirigida para restringir cierto tráfico. El tráfico se puede restringir por dirección IP, un grupo de direcciones o por tipo de protocolo.

Introducción

Las VLAN son fantásticas, definen dominios de difusión en una red de Capa 2. Los dominios de difusión suelen estar limitados por los routers porque no reenvían tramas de difusión. Los switches de Capa 2 crean dominios de difusión basados en la configuración del switch. El tráfico no puede pasar directamente a otra VLAN (entre dominios de difusión) dentro del switch o entre dos switches. Las VLAN le permiten mantener diferentes departamentos independientes entre sí. Por ejemplo, es posible que no desee que el departamento de ventas tenga ninguna implicación con el departamento de contabilidad.

La independencia es fantástica, pero ¿y si desea que los usuarios finales de las VLAN puedan rutear entre sí? Es posible que el departamento de ventas deba enviar registros o fichas de tiempo al departamento de contabilidad. Es posible que el departamento de contabilidad desee enviar notificaciones al equipo de ventas sobre sus cheques de pago o números de ventas. Esto es cuando el ruteo entre VLAN guarda el día.

Para la comunicación entre VLAN, se necesita un dispositivo de capa 3 de Interconexiones de sistemas abiertos (OSI), normalmente un router. Este dispositivo de capa 3 necesita tener una dirección de protocolo de Internet (IP) en cada interfaz VLAN y tener una ruta conectada a cada una de esas subredes IP. Los hosts de cada subred IP se pueden configurar para utilizar las respectivas direcciones IP de la interfaz VLAN como su gateway predeterminado. Una vez configurados, los usuarios finales pueden enviar un mensaje a un usuario final en la otra VLAN. Suena perfecto, ¿verdad?

Pero espera, ¿qué hay del servidor en contabilidad? Hay información confidencial en ese servidor que debe mantenerse protegida. ¡No teman, también hay una solución! Las reglas de acceso o las políticas del router serie RV34x permiten la configuración de reglas para aumentar la seguridad en la red. Las ACL son listas que bloquean o permiten el envío del tráfico hacia y desde determinados usuarios. Las reglas de acceso se pueden configurar para que estén en vigor todo el tiempo o en función de las programaciones definidas.

En este artículo se describen los pasos para configurar una segunda VLAN, ruteo entre VLAN y una ACL.

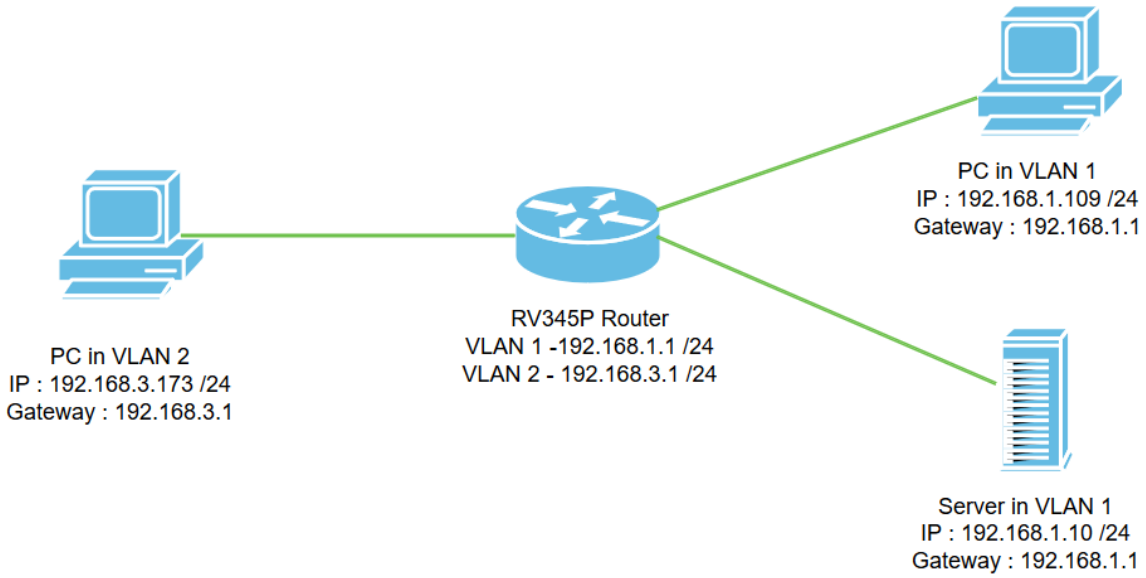
Dispositivos aplicables

- RV340
- RV340W
- RV345
- RV345P

Versión del software

- 1.0.03.16

Topología



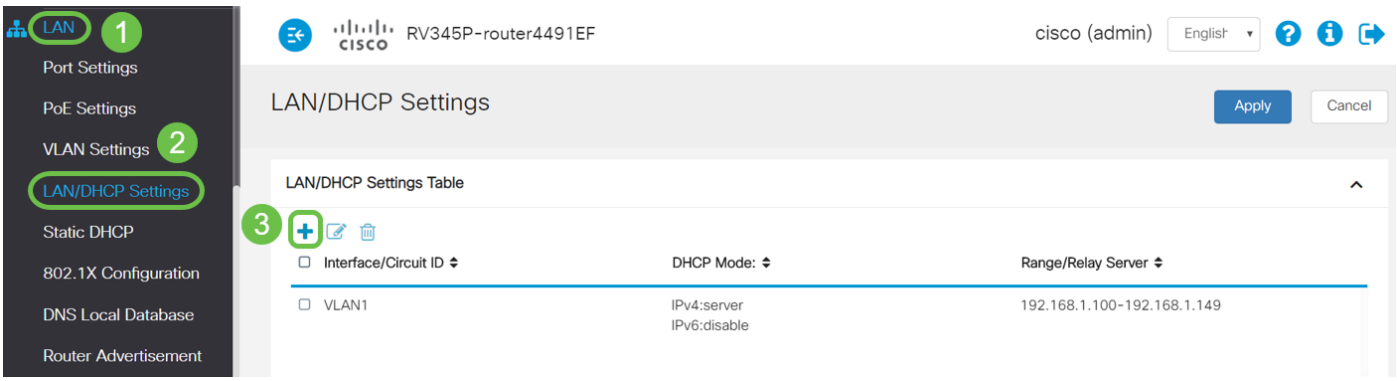
En este escenario, se habilitará el ruteo entre VLAN1 y VLAN2 para que los usuarios en estas VLAN puedan comunicarse entre sí. Como medida de seguridad, impediremos que los usuarios de VLAN2 puedan acceder al servidor VLAN1 [Protocolo de Internet versión 4 (IPv4): 192.168.1.10 /24].

Puertos del router utilizados:

- El equipo personal (PC) en VLAN1 está conectado en el puerto *LAN1*.
- El equipo personal (PC) en VLAN2 está conectado en el puerto *LAN2*.
- El servidor en VLAN1 está conectado en el puerto *LAN3*.

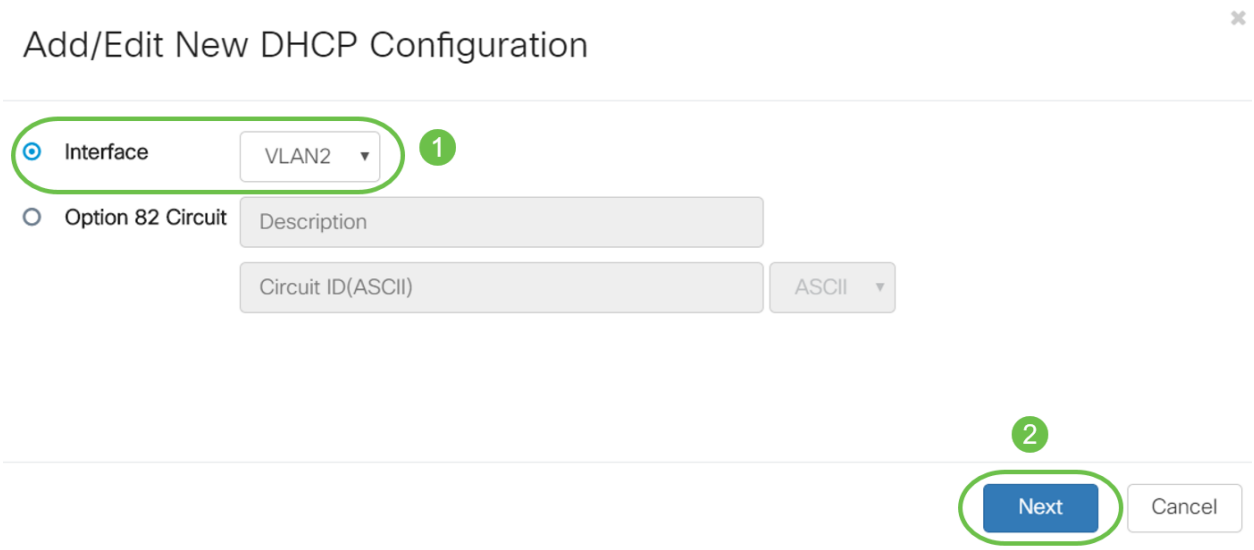
Configuración

Paso 1. Inicie sesión en la utilidad de configuración web del router. Para agregar una nueva interfaz VLAN en el router, navegue hasta **LAN > Configuración LAN/DHCP** y haga clic en el **icono más** bajo la *Tabla de Configuración LAN/DHCP*.

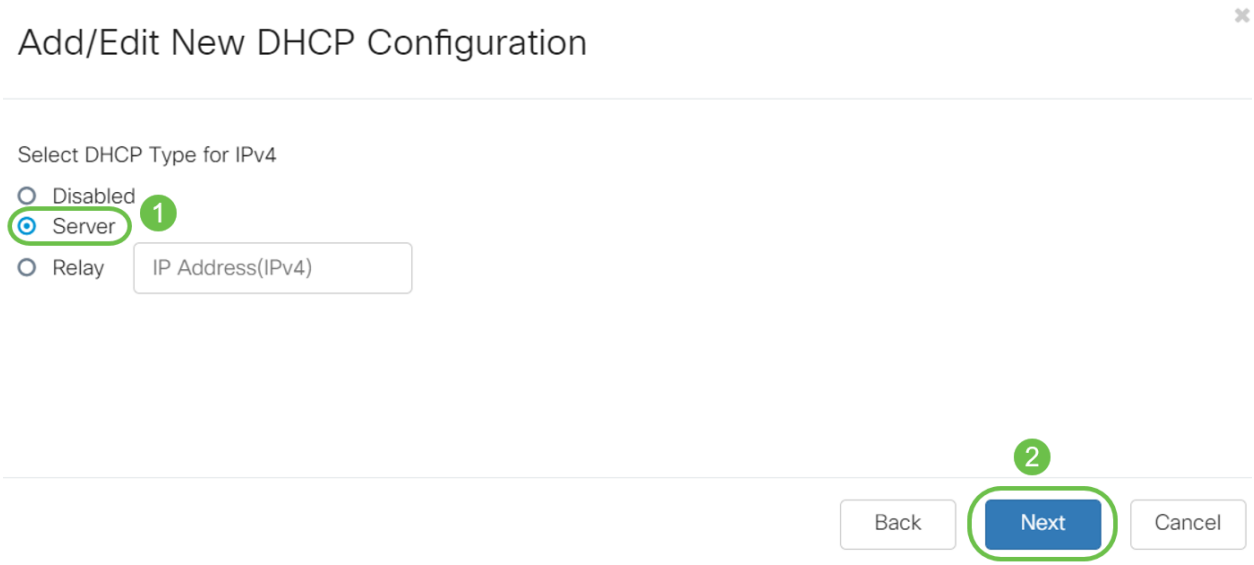


Nota: La interfaz VLAN1 se crea en el router RV34x de forma predeterminada y el servidor del protocolo de configuración dinámica de host (DHCP) para IPv4 está habilitado en él.

Paso 2. Se abrirá una nueva ventana emergente con la **interfaz** *VLAN2* seleccionada, haga clic en **Siguiente**.



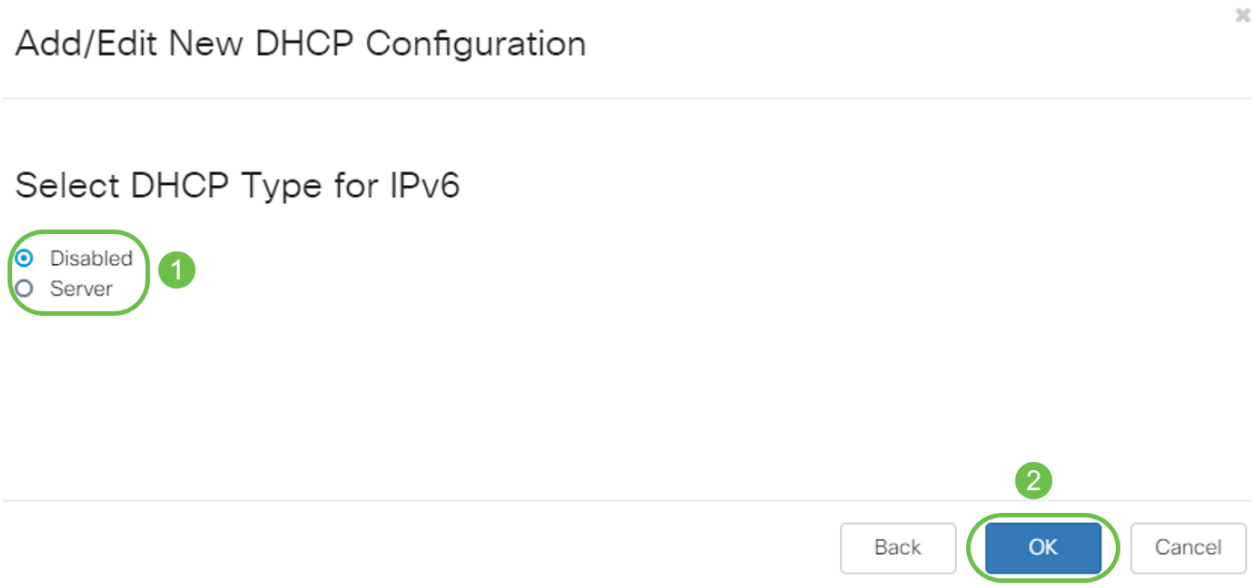
Paso 3. Para habilitar el servidor DHCP en la interfaz VLAN2, en *Seleccionar tipo DHCP para IPv4* seleccione **Servidor**. Haga clic en Next (Siguiente).



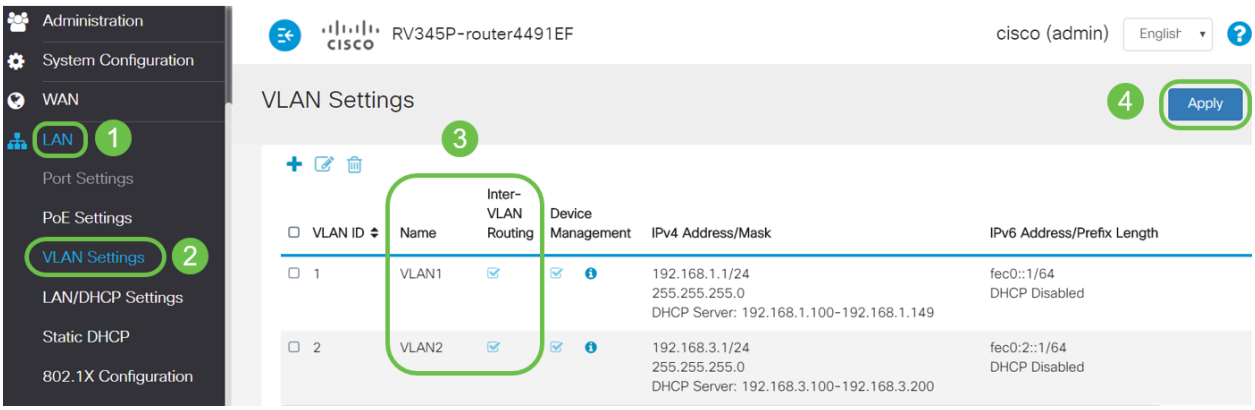
Paso 4. Ingrese los parámetros de configuración del servidor DHCP incluyendo *Client Lease Time, Range Start, Range End* y *DNS Server.* Haga clic en Next (Siguiente).

Paso 5. (Opcional) Puede inhabilitar el *tipo DHCP para IPv6* seleccionando la casilla de verificación **Disabled**, ya que este ejemplo se basa en IPv4. Click OK. La configuración del servidor DHCP ha finalizado.

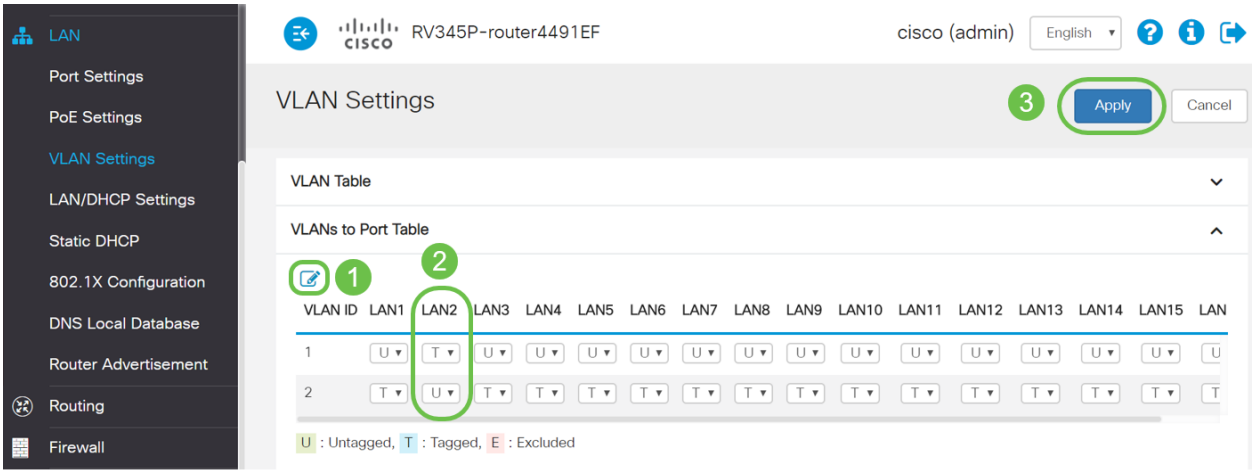
Nota: Puede utilizar IPv6.



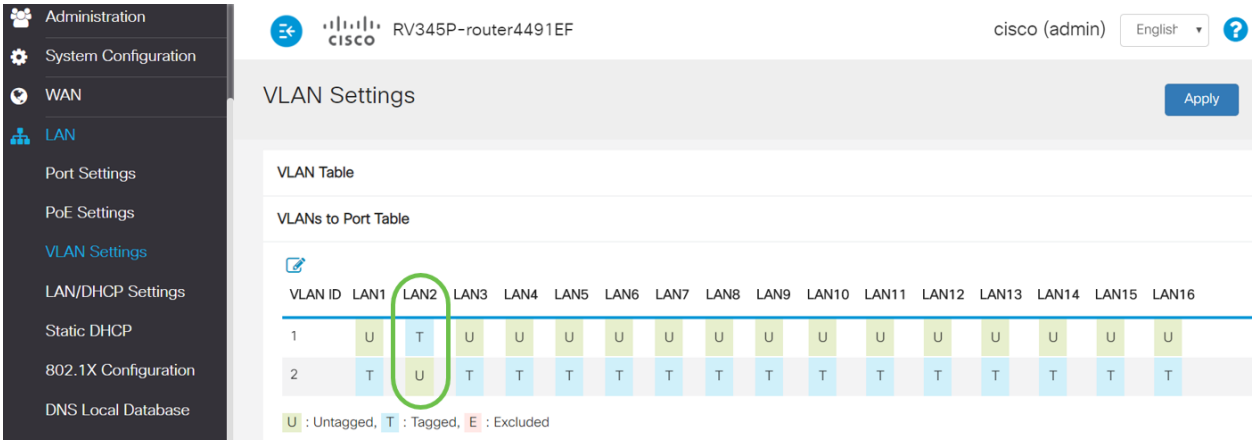
Paso 6. Navegue hasta **LAN > VLAN Settings** y verifique que *Inter-VLAN Routing* esté habilitado para las VLAN, VLAN1 y VLAN2. Esta configuración habilitará las comunicaciones entre ambas VLAN. Haga clic en Apply (Aplicar).



Paso 7. Para asignar el tráfico sin etiqueta para VLAN2 en el puerto *LAN2*, haga clic en el botón Edit bajo la opción *VLANs to Port Table*. Ahora, bajo el puerto LAN2 seleccione la opción **T** (Etiquetado) para la opción *VLAN1* y la opción *U* (No Etiquetado) para la *VLAN2* en el menú desplegable. Haga clic en **Aplicar** para guardar la configuración. Esta configuración reenviará el tráfico sin etiquetas para VLAN2 en el puerto LAN2 de modo que la tarjeta de interfaz de red (NIC) del PC, que normalmente no puede etiquetar VLAN, pueda obtener la IP DHCP de VLAN2 y formar parte de VLAN2.

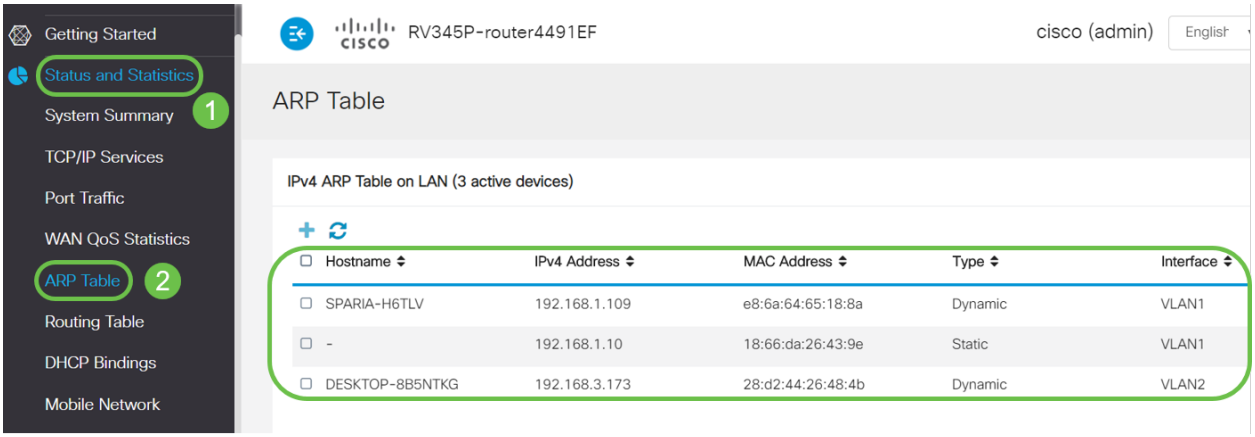


Paso 8. Verifique que la configuración de VLAN2 para el puerto *LAN2* se muestre como U *(Untagged)*. Para los puertos LAN restantes, la configuración VLAN2 será *T (Etiquetado)* y el tráfico VLAN1 será *U (Sin etiquetar)*.

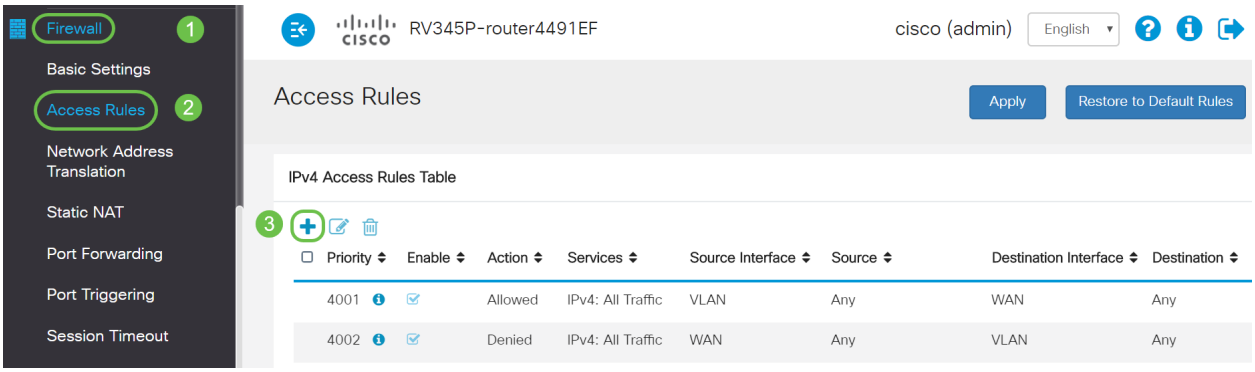


Paso 9. Navegue hasta **Status and Statistics > ARP Table** y verifique la *dirección IPv4* **dinámica para los PCs en diferentes VLAN.**

Nota: La IP del servidor en VLAN1 se ha asignado estáticamente.



Paso 10. Aplicar ACL para restringir el servidor (IPv4: 192.168.1.10/24) de los usuarios de VLAN2. Para configurar la ACL, navegue hasta **Firewall > Access Rules** y haga clic en el **icono plus** para agregar una nueva regla.



Paso 11. Configure los parámetros *de las reglas de acceso*. Para este escenario, los parámetros serán los siguientes:

Estado de la regla: Habilitar

Acción: Denegar

Servicios: Todo el tráfico

Registro: Verdadero

Interfaz de origen: VLAN2

Dirección de la fuente: cualquiera

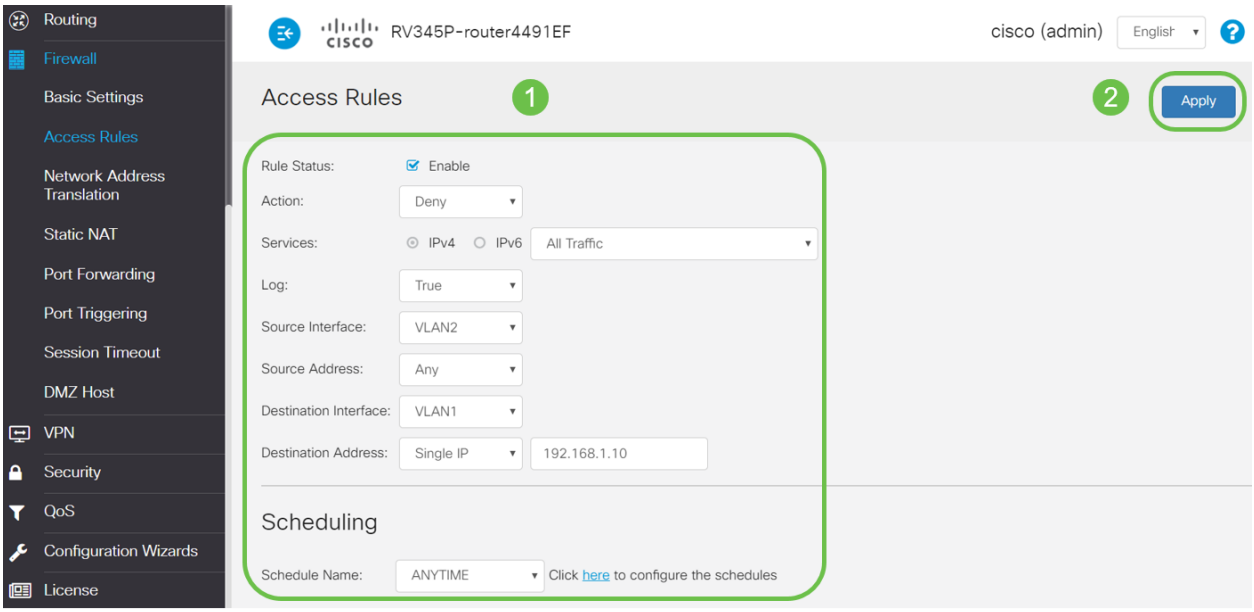
Interfaz de destino: VLAN1

dirección de destino: IP única 192.168.1.10

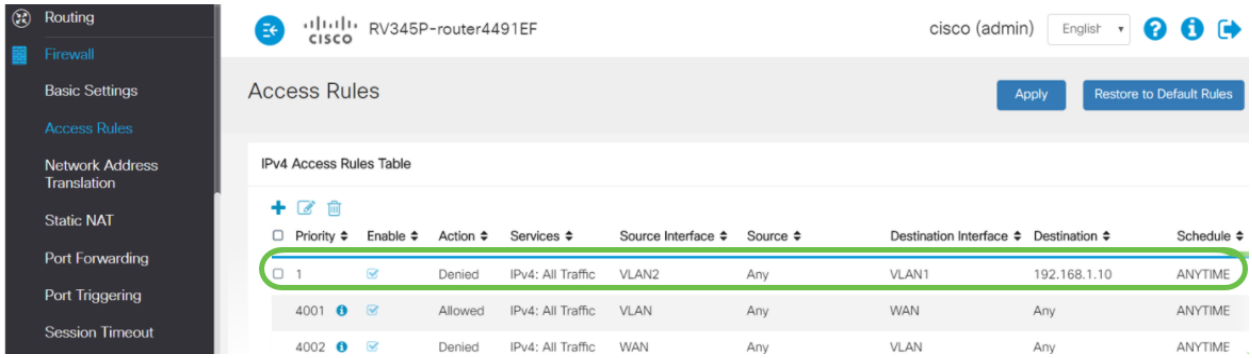
Nombre de la programación: En cualquier momento

Haga clic en Apply (Aplicar).

Nota: En este ejemplo, negamos el acceso de cualquier dispositivo desde VLAN2 al servidor y luego permitimos el acceso a los otros dispositivos en VLAN1. Sus necesidades pueden variar.



Paso 12. La lista *Reglas de acceso* mostrará lo siguiente:



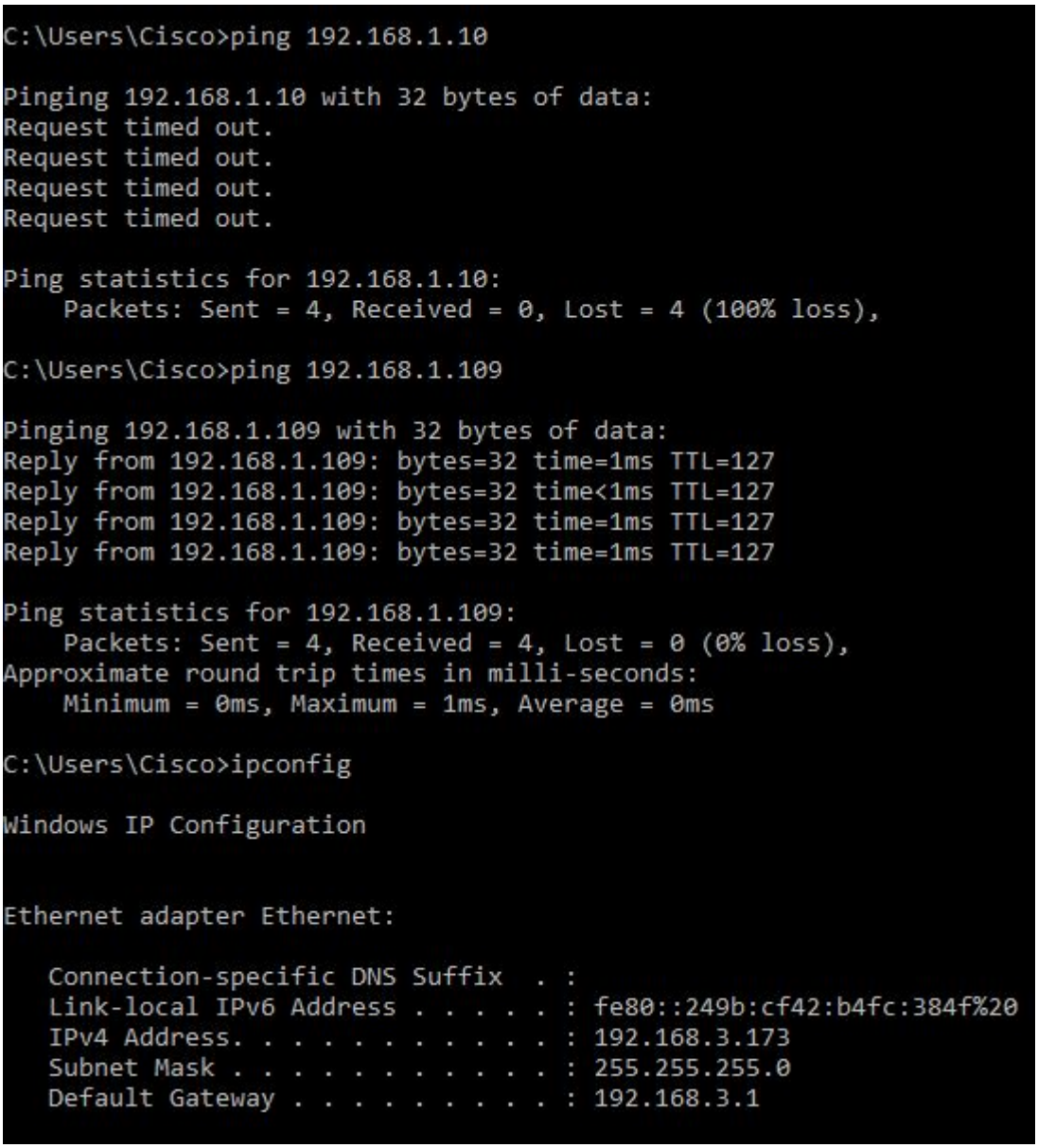
La regla de acceso se define explícitamente para restringir el acceso del servidor, 192.168.1.10, desde los usuarios de VLAN2.

Verificación

Para verificar el servicio, abra el símbolo del sistema. En las plataformas de Windows, esto se puede lograr haciendo clic en el botón Windows y, a continuación, escribiendo **cmd** en el cuadro de búsqueda inferior izquierda del equipo y seleccionando **símbolo del sistema** en el menú.

Ingrese los siguientes comandos:

- En PC (192.168.3.173) en VLAN2, haga ping en el servidor (IP: 192.168.1.10). Recibirá una notificación *de tiempo de espera agotado de la solicitud*, lo que significa que no se permite la comunicación.
- En PC (192.168.3.173) en VLAN2, haga ping en el otro PC (192.168.1.109) en VLAN1. Obtendrá una respuesta satisfactoria.



Conclusión

Ha visto los pasos necesarios para configurar el ruteo entre VLAN en un router de la serie RV34x y cómo hacer una restricción de ACL dirigida. Ahora puede tomar todo ese conocimiento y utilizarlo para crear VLAN en su red que se adapten a sus necesidades.