Configuración de la lista de control de acceso (ACL) basada en IPv6 y la entrada de control de acceso (ACE) en un switch

Objetivo

Una lista de control de acceso (ACL) es una lista de filtros de tráfico de red y acciones correlacionadas utilizadas para mejorar la seguridad. Bloquea o permite a los usuarios acceder a recursos específicos. Una ACL contiene los hosts a los que se permite o se niega el acceso al dispositivo de red.

La funcionalidad típica de ACL en IPv6 es similar a las ACL en IPv4. Las ACL determinan qué tráfico bloquear y qué tráfico reenviar en las interfaces del switch. Las ACL permiten el filtrado basado en las direcciones de origen y de destino, entrantes y salientes a interfaces específicas. Cada ACL tiene una sentencia deny implícita al final. Las reglas para las ACL se configuran en las entradas de control de acceso (ACE).

Debe utilizar las listas de acceso para proporcionar un nivel básico de seguridad para acceder a la red. Si no configura las listas de acceso en los dispositivos de red, todos los paquetes que pasan a través del switch o del router podrían estar permitidos en todas las partes de la red.

Este artículo proporciona instrucciones sobre cómo configurar ACL y ACE basadas en IPv6 en un switch.

Dispositivos aplicables

- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

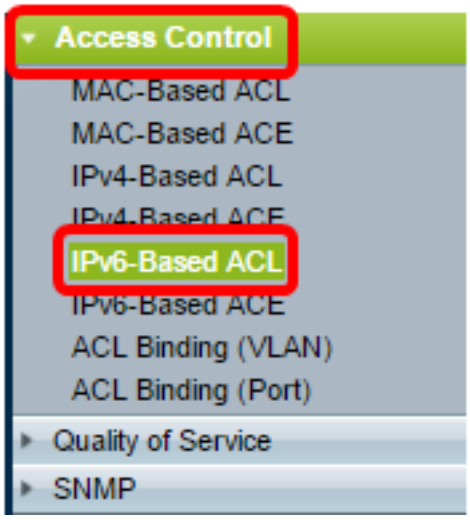
Versión del software

- 1.4.5.02 - Serie Sx500
- 2.2.5.68: Serie Sx350, Serie SG350X Y Serie Sx550X

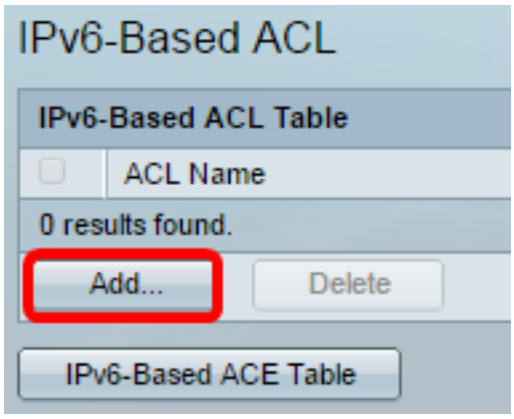
Configuración de ACE y ACL Basadas en IPv6

Configuración de ACL Basada en IPv6

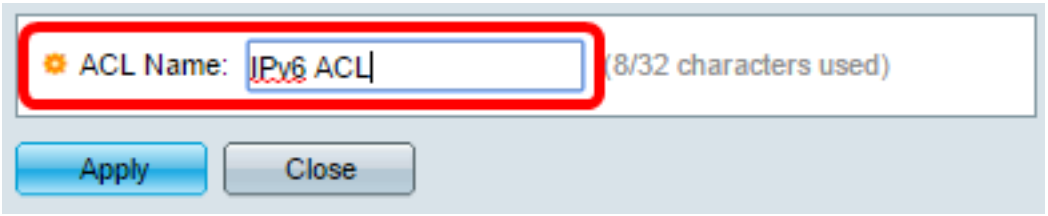
Paso 1. Inicie sesión en la utilidad basada en web y luego vaya a **Control de Acceso > ACL basada en IPv6**.



Paso 2. 'Haga clic en el botón Add (Agregar).'

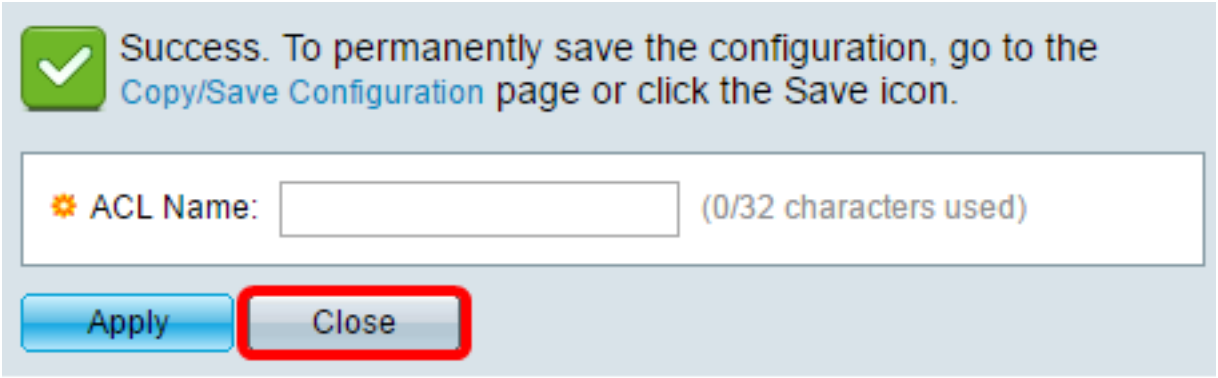


Paso 3. Ingrese el nombre de la nueva ACL en el campo *ACL Name*.



Nota: En este ejemplo, se utiliza la ACL IPv6.

Paso 4. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.



Paso 5. (Opcional) Haga clic en **Guardar** para guardar la configuración en el archivo de configuración de inicio.

Ahora debería haber configurado una ACL basada en IPv6 en su switch.

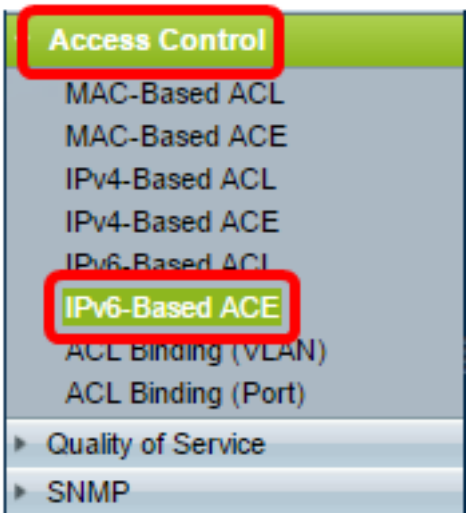
Configuración de ACE basada en IPv6

Cuando se recibe un paquete en un puerto, el switch procesa la trama a través de la primera ACL. Si el paquete coincide con un filtro ACE de la primera ACL, se realiza la acción ACE. Si el paquete no coincide con ninguno de los filtros ACE, se procesa la siguiente ACL. Si no se encuentra ninguna coincidencia con ninguna ACE en todas las ACL relevantes, el paquete se descarta de forma predeterminada.

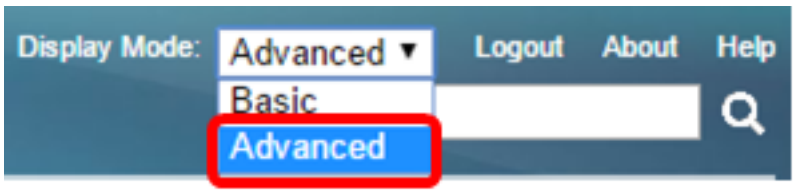
En esta situación, se creará una ACE para denegar el tráfico que se envía desde una dirección IPv6 de origen definida por el usuario específica a cualquier dirección de destino.

Nota: Esta acción predeterminada puede evitarse mediante la creación de una ACE de baja prioridad que permita todo el tráfico.

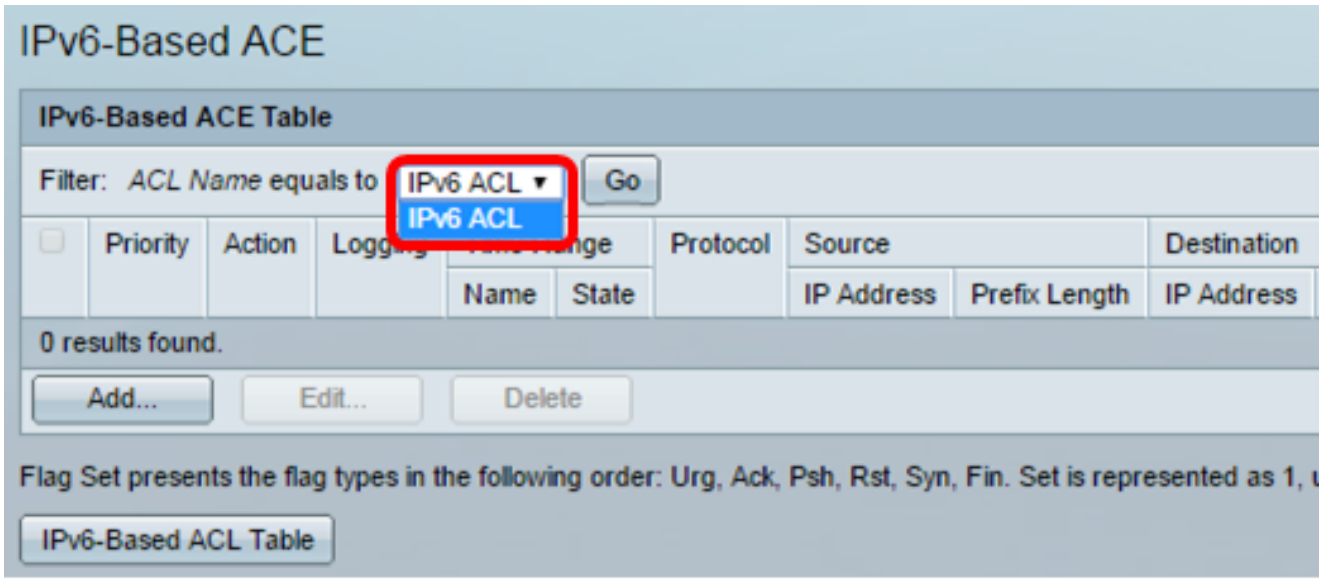
Paso 1. En la utilidad basada en web, vaya a **Access Control > IPv6 -Based ACE**.



Importante: Si tiene un switch Sx350, SG350X, Sx550X, cambie al modo avanzado seleccionando **Advanced** en la lista desplegable Display Mode en la esquina superior derecha de la página.

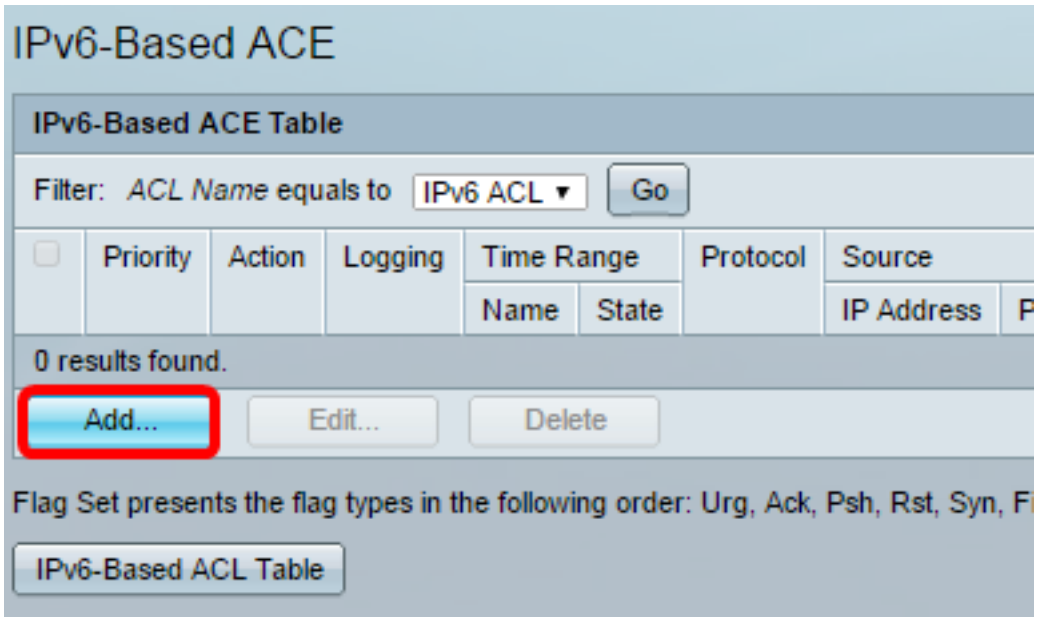


Paso 2. Elija una ACL de la lista desplegable Nombre de ACL y luego haga clic en **Ir**.



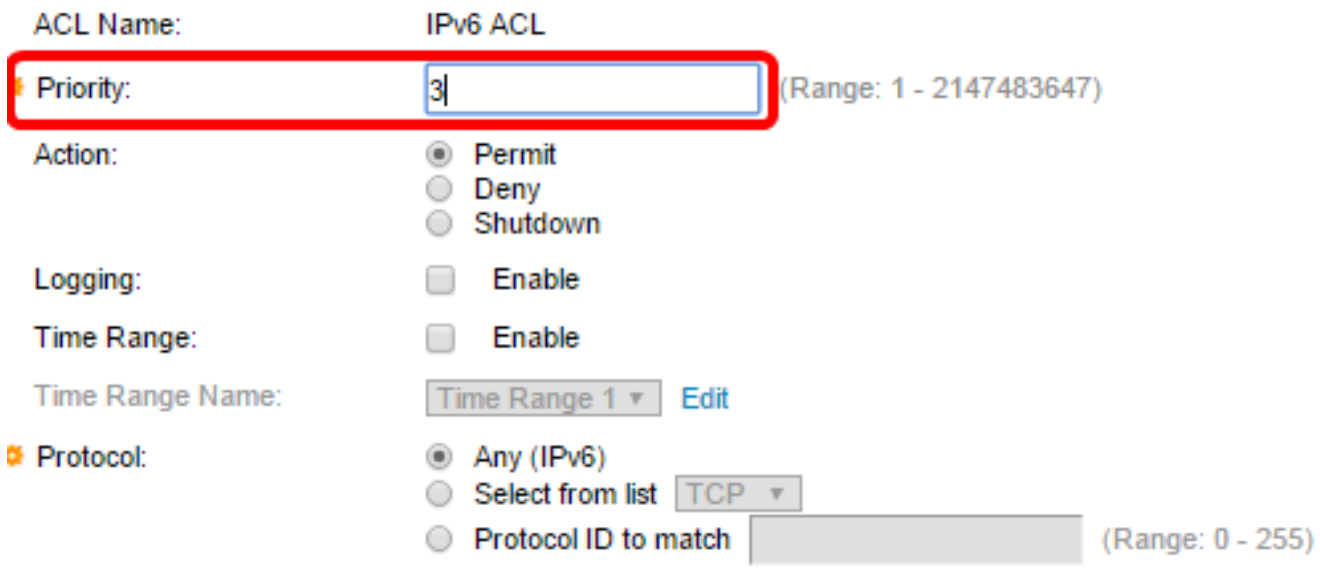
Nota: Las ACE que ya están configuradas para la ACL se mostrarán en la tabla.

Paso 3. Haga clic en el botón **Add** para agregar una nueva regla a la ACL.



Nota: El campo *ACL Name* muestra el nombre de la ACL.

Paso 4. Introduzca el valor de prioridad para ACE en el campo *Priority*. Las ACE con un valor de prioridad más alto se procesan primero. El valor 1 es la prioridad más alta. Tiene un rango de 1 a 2147483647.



Nota: En este ejemplo, se utiliza 3.

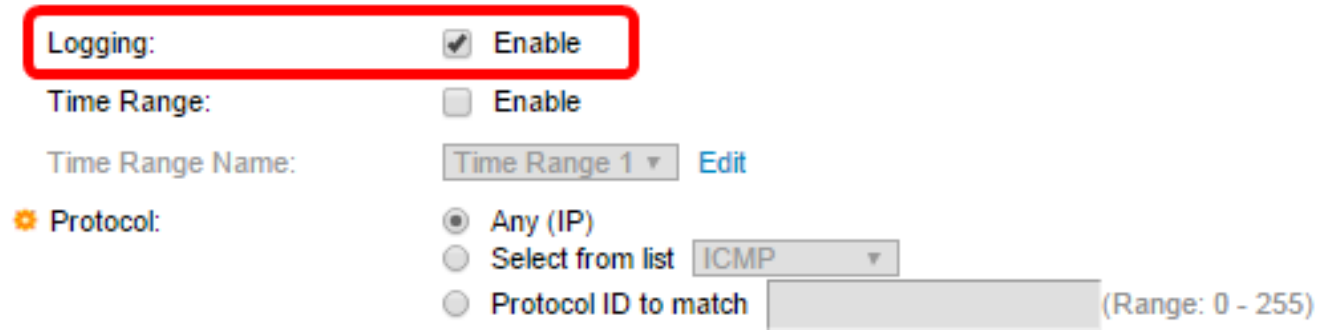
Paso 5. Haga clic en el botón de opción correspondiente a la acción deseada que se realiza cuando una trama cumple los criterios requeridos de la ACE.

Nota: En este ejemplo, se elige Permitir.

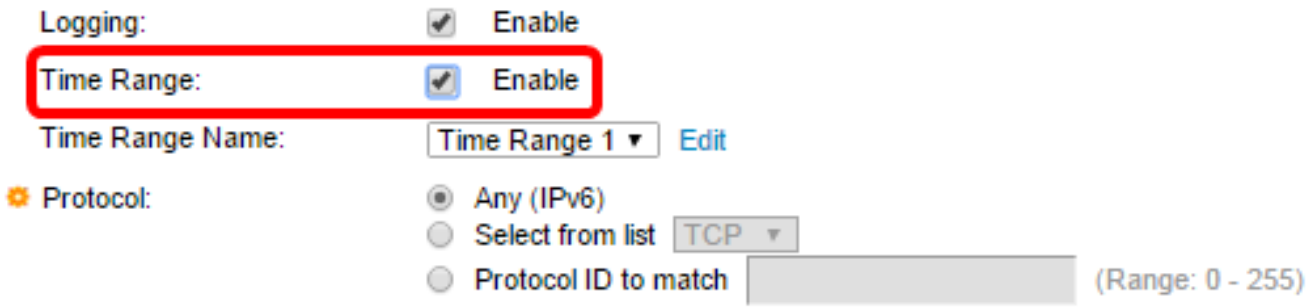
- Permiso: el switch reenvía los paquetes que cumplen los criterios requeridos de la ACE.
- Denegar: el switch descarta los paquetes que cumplen los criterios requeridos de la ACE.

Shutdown: el switch descarta los paquetes que no cumplen con los criterios requeridos de ACE e inhabilita el puerto donde se recibieron los paquetes. Los puertos desactivados se pueden reactivar en la página Port Settings (Configuración de puerto).

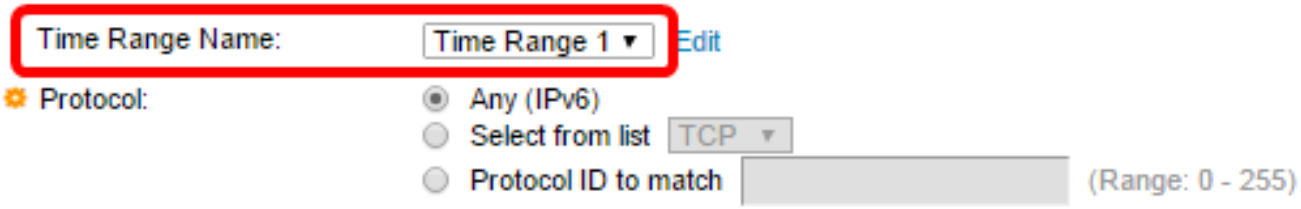
Paso 6. (Opcional) Marque la casilla de verificación **Enable** Logging para habilitar el registro de flujos ACL que coincidan con la regla ACL.



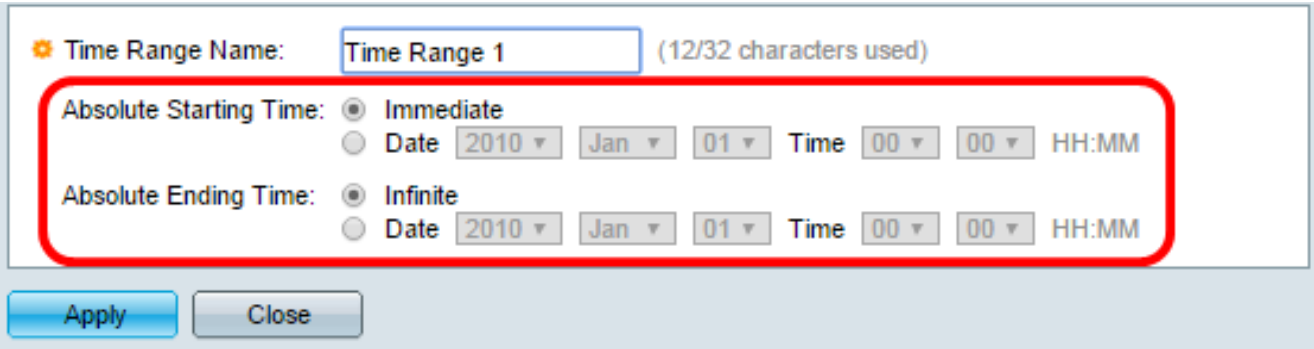
Paso 7. (Opcional) Marque la casilla de verificación **Enable** Time Range para permitir que se configure un rango de tiempo en ACE. Los rangos de tiempo se utilizan para limitar la cantidad de tiempo que una ACE está en vigor. Si esto se deja desactivado, la ACE funciona en cualquier momento.



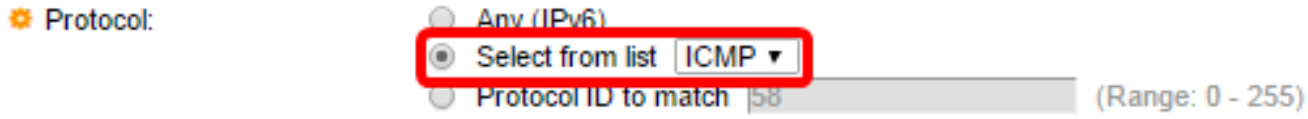
Paso 8. (Opcional) En la lista desplegable Nombre de rango de tiempo, elija un rango de tiempo para aplicar a la ACE.



Nota: Puede hacer clic en **Editar** para navegar y crear un intervalo de tiempo en la página Intervalo de tiempo.



Paso 9. Elija un tipo de protocolo en el área Protocol . La ACE se creará en función de un protocolo o ID de protocolo específicos.

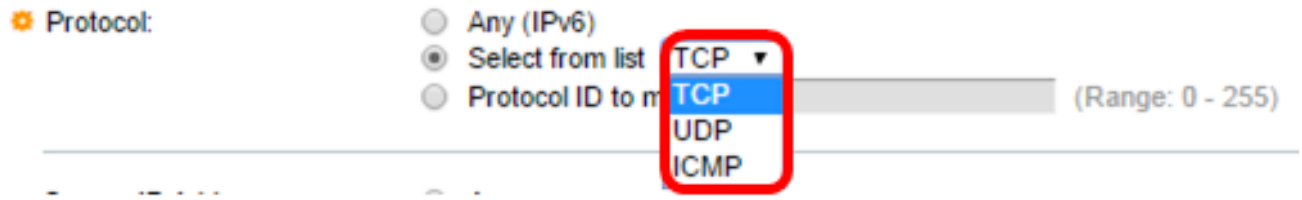


Las opciones son:

- Any (IP): esta opción configurará la ACE para aceptar todos los protocolos IP.
- Seleccionar de la lista: esta opción le permitirá elegir un protocolo de una lista desplegable. Si prefiere esta opción, vaya directamente al Paso 10.
- ID de protocolo para que coincida: esta opción le permitirá introducir una ID de protocolo. Si prefiere esta opción, vaya directamente al Paso 11.

Nota: En este ejemplo, se elige Seleccionar de la lista.

Paso 10. (Opcional) Si selecciona Seleccionar de la lista del paso 9, elija un protocolo de la lista desplegable.

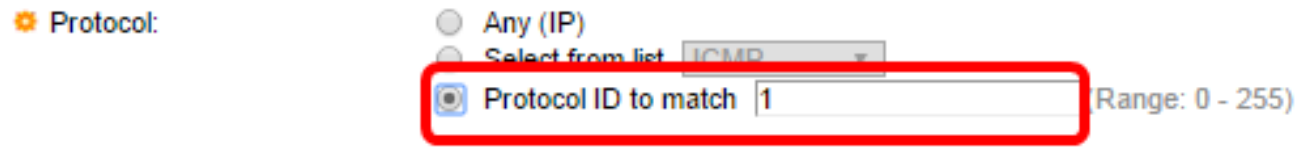


Las opciones son:

- TCP: el protocolo de control de transmisión (TCP) permite que dos hosts se comuniquen e intercambien secuencias de datos. TCP garantiza la entrega de paquetes y garantiza que los paquetes se transmiten y reciben en el orden en que se enviaron.
- UDP: el protocolo de datagramas de usuario (UDP) transmite los paquetes pero no garantiza su entrega.
- ICMP: hace coincidir paquetes con el protocolo de mensajes de control de Internet (ICMP).

Nota: En este ejemplo, se utiliza TCP.

Paso 11. (Opcional) Si ha seleccionado Protocol ID (ID de protocolo) para que coincida en el paso 9, introduzca el ID de protocolo en el *ID de protocolo para que coincida* en el campo.



Nota: En este ejemplo, se utiliza 1.

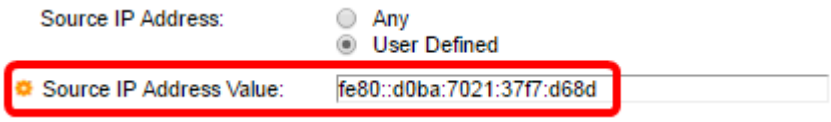
Paso 12. Haga clic en el botón de opción que se corresponda con los criterios deseados de ACE en el área Dirección IP de Origen.

Las opciones son:

- Any: todas las direcciones IPv6 de origen se aplican a ACE.
- Definido por el Usuario: introduzca una dirección IP y una máscara de comodín IP que se aplicarán a la ACE en los campos *Valor de la dirección IP de origen y Longitud del prefijo IP de origen*.

Nota: En este ejemplo, se elige Definido por el usuario. Si selecciona Any (Cualquiera), vaya al Paso 15.

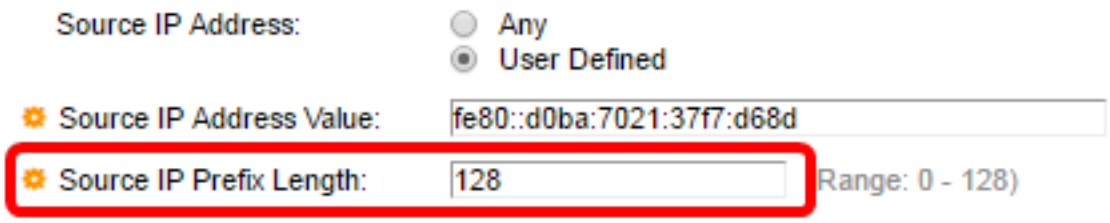
Paso 13. Ingrese la dirección IP de origen en el campo *Source IP Address Value* .



Nota: En este ejemplo, se utiliza fe80::d0ba:7021:37f7:d68d.

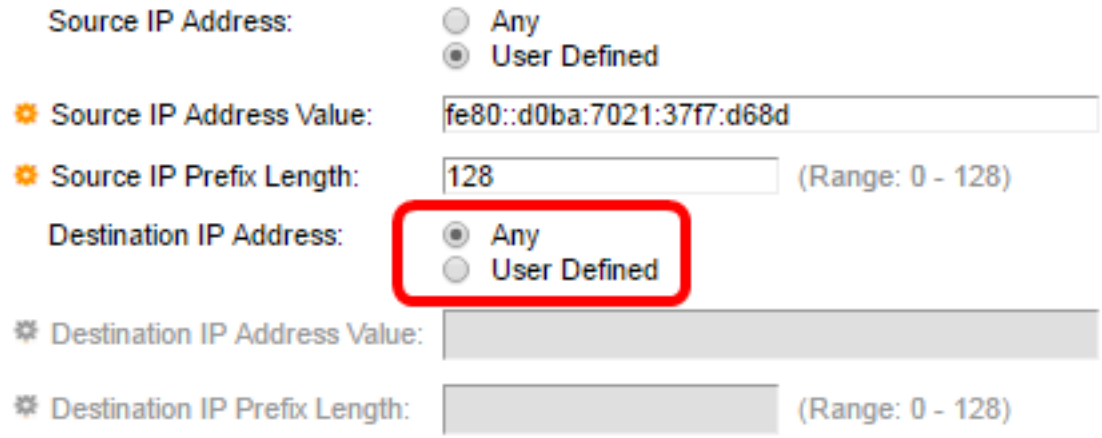
Paso 14. Ingrese la longitud del prefijo IP de origen en el campo *Longitud del prefijo IP de*

origen.



Nota: En este ejemplo, se utiliza 128.

Paso 15. Haga clic en el botón de opción que se corresponda con los criterios deseados de ACE en el área DestinationIP Address (Dirección IP de destino).

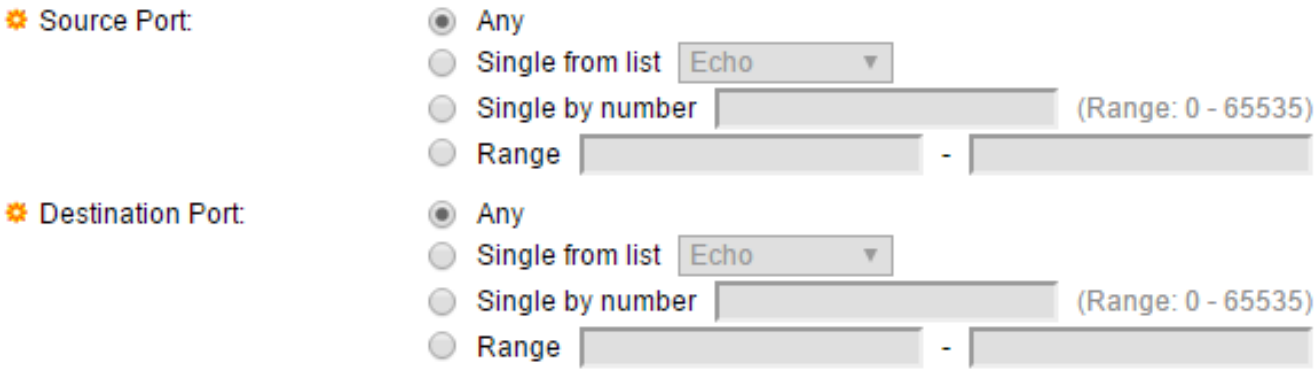


Las opciones son:

- Any: todas las direcciones IPv6 de destino se aplican a ACE.
- Definido por el Usuario: introduzca una dirección IP y una máscara comodín IP que se aplicarán a la ACE en los campos *Valor de la dirección IP de destino y Longitud de IPPrefix*.

Nota: En este ejemplo, se elige Any (Cualquiera). Si elige esta opción, la ACE que se creará permitirá que el tráfico ACE que provenga de la dirección IPv6 especificada a cualquier destino.

Paso 16. (Opcional) Haga clic en un botón de opción del área Puerto de origen. El valor predeterminado es Any (Cualquiera).



- Any: haga coincidir con todos los puertos de origen.
- Único de la lista: puede elegir un único puerto de origen TCP/UDP con el que coincidan los paquetes. Este campo sólo está activo si se elige 800/6-TCP o 800/17-UDP en el menú

desplegable Seleccionar de la lista.

- Único por número: puede elegir un único puerto de origen TCP/UDP al que coincidan los paquetes. Este campo sólo está activo si se elige 800/6-TCP o 800/17-UDP en el menú desplegable Seleccionar de la lista.
- Rango: puede elegir un rango de puertos de origen TCP/UDP a los que se corresponde el paquete. Hay ocho intervalos de puertos diferentes que se pueden configurar (compartidos entre los puertos de origen y de destino). Los protocolos TCP y UDP tienen cada uno ocho intervalos de puertos.

Paso 17. (Opcional) Haga clic en un botón de opción en el área Puerto de destino. El valor predeterminado es Any (Cualquiera).

- Any — Coincide con todos los puertos de origen
- Único de la lista: puede elegir un único puerto de origen TCP/UDP con el que coincidan los paquetes. Este campo sólo está activo si se elige 800/6-TCP o 800/17-UDP en el menú desplegable Seleccionar de la lista.
- Único por número: puede elegir un único puerto de origen TCP/UDP al que coincidan los paquetes. Este campo sólo está activo si se elige 800/6-TCP o 800/17-UDP en el menú desplegable Seleccionar de la lista.
- Rango: puede elegir un rango de puertos de origen TCP/UDP a los que se corresponde el paquete. Hay ocho intervalos de puertos diferentes que se pueden configurar (compartidos entre los puertos de origen y de destino). Los protocolos TCP y UDP tienen cada uno ocho intervalos de puertos.

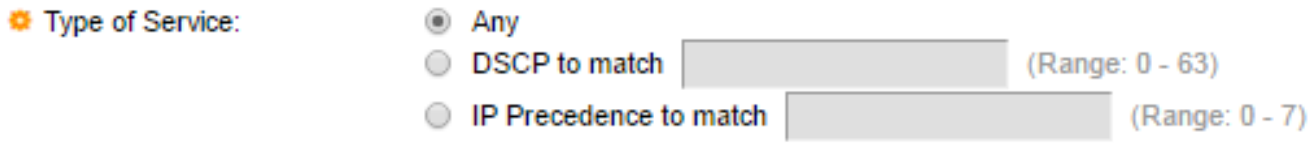
Paso 18. (Opcional) En el área TCP Flags, elija uno o más indicadores TCP con los que filtrar los paquetes. Los paquetes filtrados se reenvían o se descartan. El filtrado de paquetes por indicadores TCP aumenta el control de paquetes, lo que aumenta la seguridad de la red.

- Establecer: Coincida si el indicador está establecido.
- Unset: Coincida si el indicador no está configurado.
- No se preocupe: ignore el indicador TCP.

Los indicadores TCP son:

- Urg: este indicador se utiliza para identificar los datos entrantes como Urgente.
- Ack: este indicador se utiliza para confirmar la recepción correcta de los paquetes.
- Psh: este indicador se utiliza para garantizar que los datos reciben la prioridad (que merece) y se procesan en el extremo de envío o recepción.
- Rst: este indicador se utiliza cuando llega un segmento que no está destinado a la conexión actual.
- Syn: este indicador se utiliza para las comunicaciones TCP.
- Fin: este indicador se utiliza cuando la comunicación o la transferencia de datos finaliza.

Paso 19. (Opcional) Haga clic en el tipo de servicio del paquete IP del área Tipo de servicio.



Las opciones son:

- Any: puede ser cualquier tipo de servicio para la congestión del tráfico.
- DSCP a coincidencia: el punto de código de servicios diferenciados es un mecanismo para clasificar y administrar el tráfico de red. Se utilizan seis bits (0-63) para seleccionar el comportamiento por salto que experimenta un paquete en cada nodo.
- Precedencia IP que debe coincidir: la precedencia IP es un modelo de tipo de servicio (TOS) que utiliza la red para ayudar a proporcionar los compromisos de calidad de servicio (QoS) adecuados. Este modelo utiliza los tres bits más significativos del byte de tipo de servicio en el encabezado IP, como se describe en RFC 791 y RFC 1349. La palabra clave con valores de preferencia IP es la siguiente:

    - 0 — para rutina

    - 1 — para prioridad

    - 2 — para

    - 3 — para flash

    - 4: para la anulación de flash

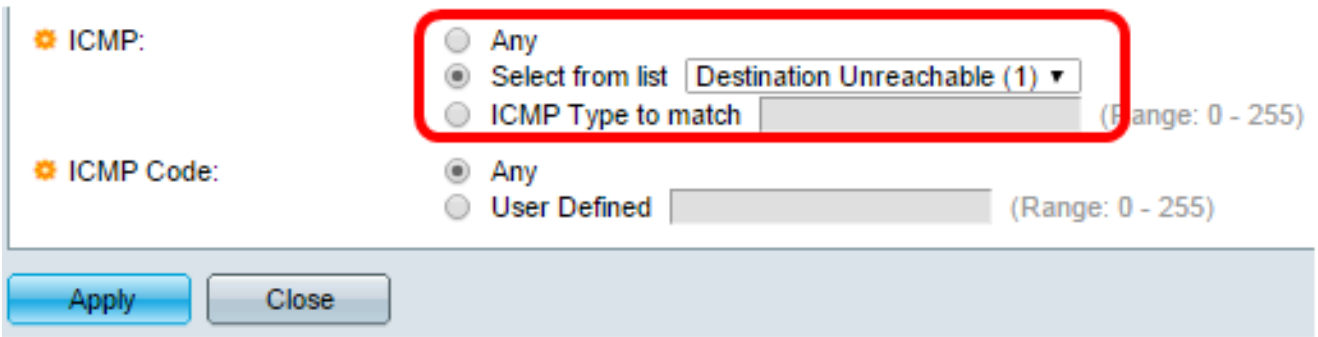
    - 5 — para críticas

    - 6 — para internet

    - 7: para la red

Nota: En este ejemplo, se elige Any (Cualquiera).

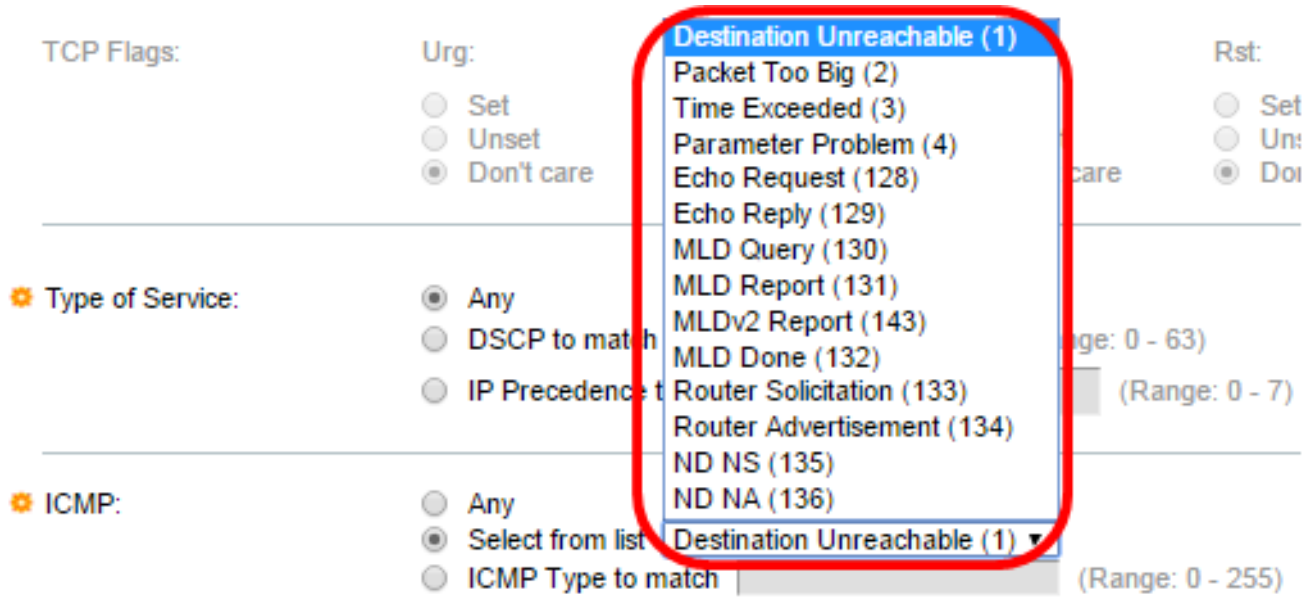
Paso 20. (Opcional) Si el protocolo IP de la ACL es ICMP, haga clic en el tipo de mensaje ICMP utilizado para fines de filtrado. Elija el tipo de mensaje por nombre o introduzca el número de tipo de mensaje:



- Any: se aceptan todos los tipos de mensajes.
- Seleccionar de la lista: puede elegir el tipo de mensaje por nombre.
- Tipo ICMP que debe coincidir: el número de tipo de mensaje que se utilizará para fines de filtrado.

Nota: En este ejemplo, se elige Seleccionar de la lista.

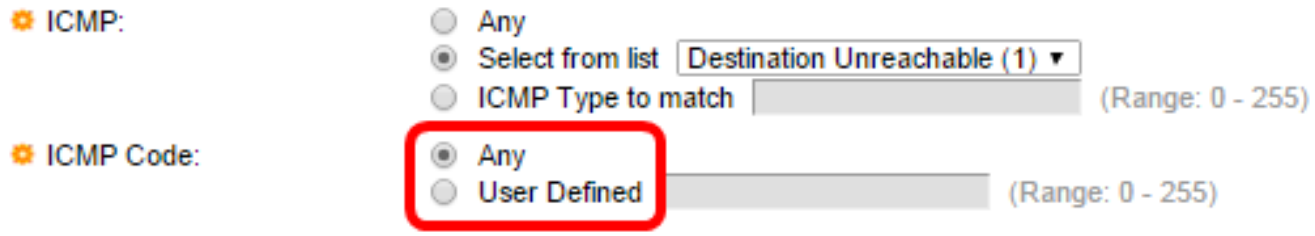
Paso 21. (Opcional) Si selecciona Seleccionar de la lista en el Paso 20, elija los mensajes de control que desea filtrar de las opciones posibles en la lista desplegable:



- Destino inalcanzable (1): el host o su gateway lo generan para informar al cliente de que el destino es inalcanzable por algún motivo (Ejemplo: Error de red o host inalcanzable).
- Paquete demasiado grande (2): el tamaño del datagrama excede la MTU dada.
- Tiempo excedido (3): un gateway genera este dato para informar al origen de un datagrama descartado debido a que el campo de tiempo de vida alcanza el cero.
- Problema del parámetro (4): se genera como respuesta para cualquier error que no esté cubierto específicamente por otro mensaje ICMP.
- Solicitud de eco (128): es un ping, cuyos datos se espera recibir de nuevo en una respuesta de eco.
- Respuesta de eco (129): se genera en respuesta a una solicitud de eco.
- Consulta MLD (130): se utiliza para saber qué direcciones multicast tienen receptores en un link adjunto. Escriba 130 en decimal.
- Informe MLD (131): se genera cuando la dirección multidifusión IPv6 a la que escucha el remitente del mensaje.
- Informe MLD v2 (143): es igual que Informe MLD con la versión 2.
- MLD Finalizado (132): cuando el host abandona un grupo, envía un mensaje de receptor multicast a los routers multicast de la red.
- Solicitud de router (133): es un mensaje de detección de router. Los hosts descubren las direcciones de sus routers vecinos simplemente cuando escuchan anuncios. El valor predeterminado es 224.0.0.2 para multicast, de lo contrario es 255.255.255.255.
- Anuncio de router (134): el router retransmite periódicamente un anuncio de router desde cada una de sus interfaces de multidifusión y anuncia las direcciones IP de esa interfaz.
- ND NS (135): los mensajes son originados por los nodos para solicitar la dirección de capa de link de otro nodo y también para funciones como la detección de direcciones duplicadas y la detección de inaccesibilidad de vecinos.
- ND NA (136): los mensajes se envían en respuesta a los mensajes NS. Si un nodo cambia su dirección de capa de link, puede enviar un NA no solicitado para anunciar la nueva dirección.

Paso 22. (Opcional) Los mensajes ICMP pueden tener un campo de código que indica cómo

manejar el mensaje. Esto se habilita si elige el protocolo ICMP en el Paso 10. Haga clic en una de las siguientes opciones para configurar si desea filtrar este código:

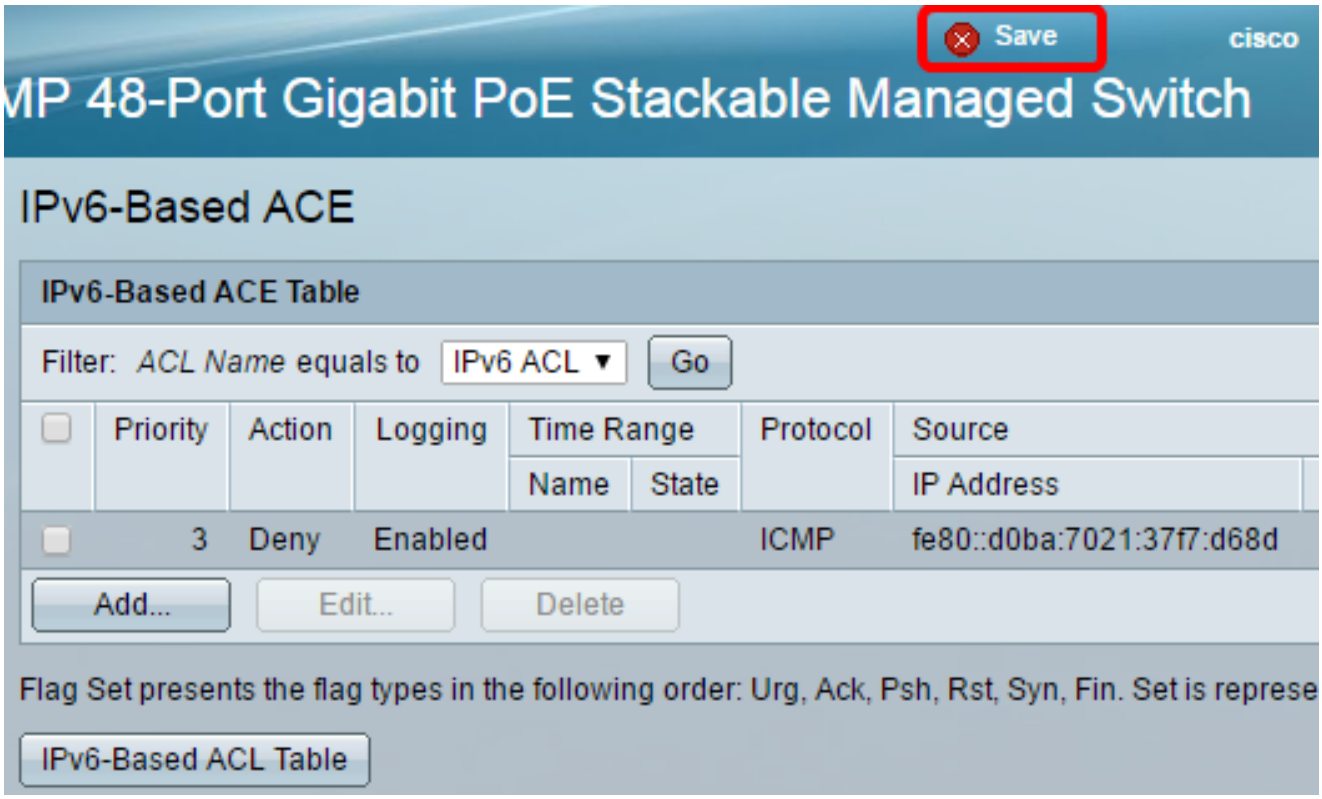


- Any: acepte todos los códigos.
- Definido por el usuario: puede introducir un código ICMP con fines de filtrado.

Nota: En este ejemplo, se elige Any (Cualquiera).

Paso 23. Haga clic en **Aplicar** y luego haga clic en **Cerrar**. La ACE se crea y se asocia al nombre de la ACL.

Paso 24. Haga clic en **Guardar** para guardar la configuración en el archivo de configuración de inicio.



Ahora debería haber configurado una ACE basada en IPv6 en su switch.