Configuración de listas de acceso basadas en IPv4 en los switches gestionados de la serie 200/300

Objetivo

Las listas de acceso son reglas que se pueden aplicar para permitir o denegar un flujo de tráfico específico en la red, lo que aporta más seguridad y aumenta el rendimiento general de la red.

El objetivo de este documento es mostrarle cómo configurar listas de acceso basadas en IPv4 en los 200/300 Series Managed Switches.

Dispositivos aplicables

·Switches gestionados serie SF/SG 200 y SF/SG 300

Versión del software

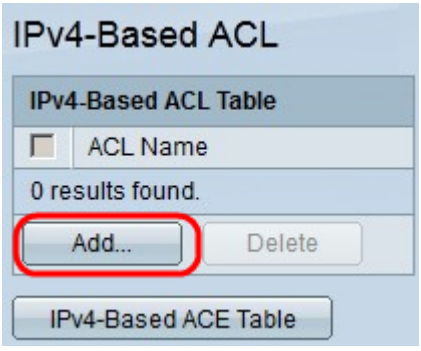
•1.3.0.62

Configuración de ACL y ACE basadas en IPv4

ACL basadas en IPv4

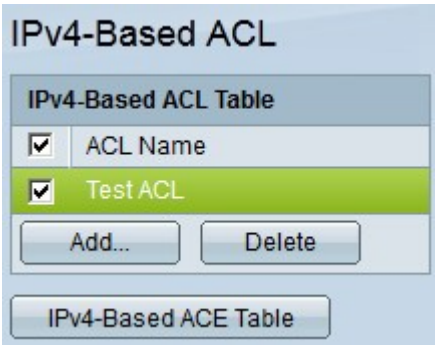
Paso 1. Inicie sesión en la utilidad de configuración web y elija **Access Control > IPv4-Based ACL**. Se abre la página *ACL basada en IPv4*.

Paso 2. Haga clic en **Agregar** para agregar una nueva lista de acceso.



Paso 3. En el campo *ACL Name*, ingrese un nombre para la nueva lista de acceso.

Paso 4. Haga clic en **Apply** para guardar la lista de acceso.



Paso 5. (Opcional) Para eliminar una lista de acceso, active la casilla de verificación de la lista de acceso que desea eliminar y haga clic en **Eliminar**.

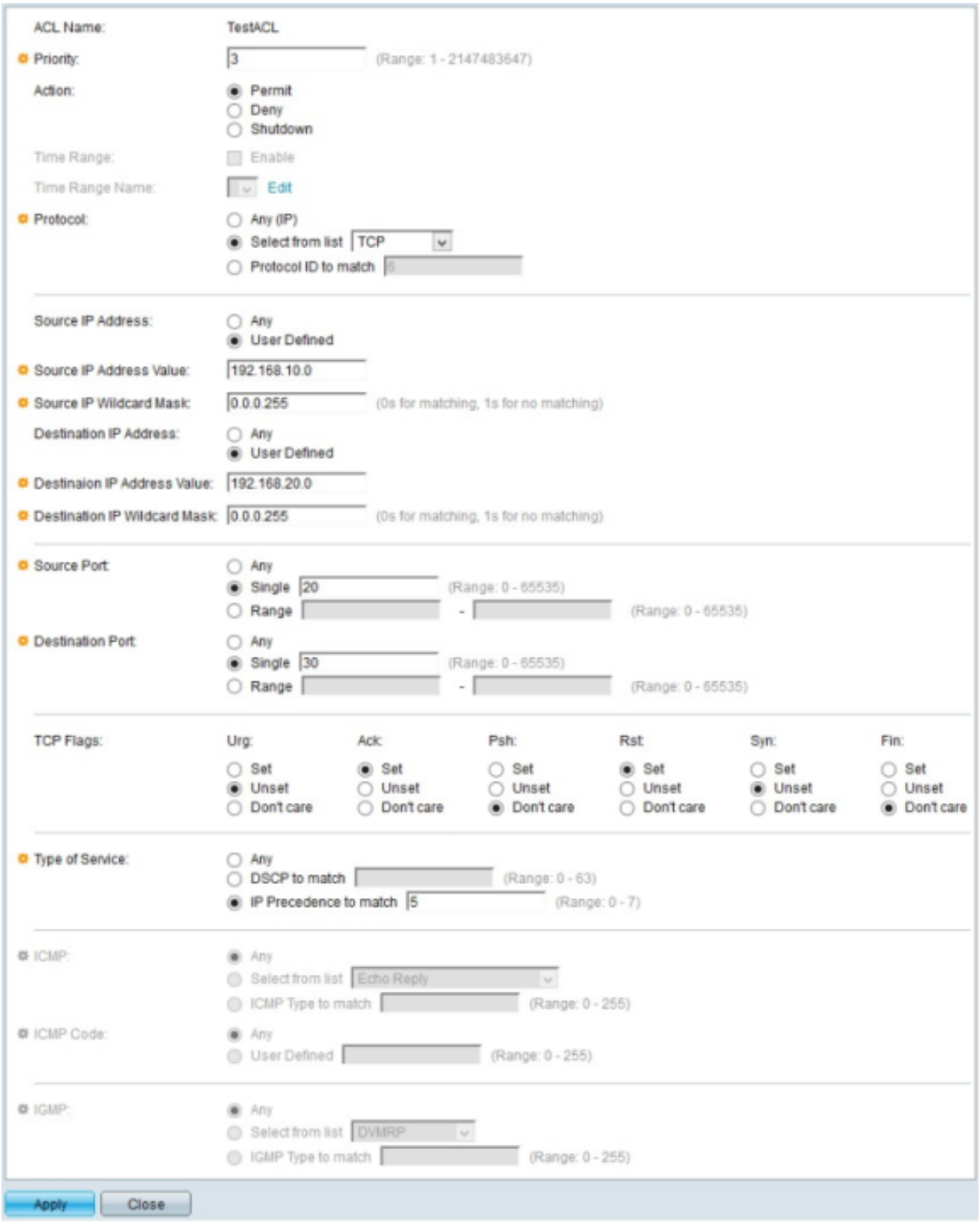
ACE basadas en IPv4

Para administrar una ACE en una ACL, se deben seguir los siguientes pasos.

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Access Control > IPv4-Based ACEs**. Se abre la página *IPv4-Based ACE*.

Paso 2. En la lista desplegable *Filtrar: Nombre de ACL igual a*, seleccione la lista de acceso a la que desea asignar una regla de acceso.

Paso 3. Haga clic en Add (Agregar). Aparece la ventana *Add IP-Based ACE*.



Paso 4. Introduzca la prioridad de la ACE en el campo *Priority*. La ACE con la prioridad más alta se procesa primero. La prioridad más alta es el 1. Tiene un rango de 1 a 2147483647.

Paso 5. En el campo *Acción*, haga clic en el botón de opción de la acción que desea que realice esta regla de acceso. Las opciones disponibles son:

·Permitir: reenvía los paquetes filtrados por la ACE actual.

·Denegar: descarta los paquetes filtrados por la ACE actual.

·Apagar: descarta los paquetes filtrados por la ACE actual e inhabilita el puerto desde el que se recibieron los paquetes.

Paso 6. En el campo *Protocol*, haga clic en el botón de opción del protocolo que desea agregar a la ACE. La ACE se configura para todos los protocolos de red enrutados para filtrar los paquetes a medida que éstos pasan a través de un router. Las opciones disponibles son:

· Cualquiera: elige cualquiera de los protocolos ACE basados en IPv4.

·Seleccionar de la lista: elija el protocolo que desee en la lista desplegable.

·Protocol ID to match: esta opción le permite introducir el ID de protocolo que desea utilizar.

Paso 7. En el campo *Source IP Address*, haga clic en una de las opciones disponibles como dirección IP de origen:

·Cualquiera: esta opción aplica la regla de acceso a cualquiera de las direcciones IP disponibles en un segmento de red específico.

·User Defined (Definido por el usuario): esta opción permite introducir una dirección IP específica.

- Valor de dirección IP de origen: en este campo, introduzca la dirección IP de origen.

- Máscara comodín IP de origen: en este campo, introduzca la máscara comodín de la dirección IP de origen. La máscara comodín le permite especificar a qué host de la dirección IP de origen se aplica esta lista de acceso.

Paso 8. En el campo *Destination IP Address*, haga clic en una de las opciones disponibles como dirección IP de destino:

·Cualquiera: esta opción aplica la regla de acceso a cualquiera de las direcciones IP disponibles en un segmento de red específico.

·Definido por el usuario: esta opción permite introducir una dirección IP específica para aplicar la regla de acceso:

- Valor de dirección IP de destino: en este campo, introduzca la dirección IP de destino.

- Destination IP Wildcard Mask (Máscara comodín de IP de destino): en este campo, introduzca la máscara comodín de la dirección IP de destino. La máscara comodín le permite especificar a qué hosts de la dirección IP de destino se aplica esta lista de acceso.

Paso 9. El campo *Source Port* se habilita solamente cuando elige TCP o UDP del Paso 5. Haga clic en el botón de opción de una de las opciones disponibles para elegir el puerto de origen:

·Any: esta opción acepta cualquier puerto de origen.

·Single: esta opción permite introducir un valor de puerto de origen único.

·Rango: esta opción le permite introducir un rango de puertos de origen disponibles.

Paso 10. El campo *Puerto de destino* se habilita solamente cuando elige TCP o UDP del Paso 5. Haga clic en el botón de opción de una de las opciones disponibles para elegir el puerto de destino:

·Any: esta opción acepta cualquier puerto de destino.

·Single: esta opción permite introducir un único valor de puerto de destino.

·Rango: esta opción le permite introducir un rango de puertos de destino disponibles.

Paso 11. El campo *Indicadores TCP* sólo se habilita si selecciona TCP en el paso 5. Haga clic en uno de los botones de opción de cada indicador para elegir el estado en el que desea activar la regla de acceso:

·Urg: este indicador identifica los datos entrantes como urgentes.

·Ack: este indicador se utiliza para confirmar la recepción de paquetes con éxito.

·Psh: este indicador se utiliza para garantizar que los datos tienen la prioridad correcta y se procesan en el extremo de envío o recepción.

·Rst: este indicador se utiliza cuando una conexión recibe un segmento incorrecto.

·Syn: este indicador se utiliza para las comunicaciones TCP.

·Fin: este indicador se utiliza cuando finaliza la comunicación o la transferencia de datos.

Paso 12. En el campo *Type of Service*, haga clic en uno de los botones de opción disponibles para elegir un tipo de servicio para el paquete IP:

·Cualquiera: esta opción elige cualquier tipo de servicio.

·DSCP para comparar: elija esta opción para implementar el punto de código de servicio diferenciado (DSCP) como tipo de servicio. DSCP es un mecanismo para clasificar y administrar el tráfico de red. Introduzca el valor DSCP que desea aplicar a la regla de acceso.

·Precedencia de IP a igualar: la red actual utiliza este tipo de servicio para proporcionar la QoS (calidad de servicio) correcta. Introduzca el valor que desea aplicar a la regla de acceso.

Paso 13. El campo *ICMP (Internet Control Message Protocol)* se habilita solamente cuando elige ICMP en el Paso 5. ICMP se utiliza para enviar mensajes de error cuando un servicio no está disponible o para probar la conectividad. Haga clic en uno de los botones de opción disponibles para filtrar los tipos de mensajes ICMP:

·Cualquiera: puede ser cualquiera de los mensajes de error o de consulta.

·Selecciónelo en la lista: elija cualquiera de los mensajes de control permitidos en la lista desplegable.

·Tipo de ICMP que debe coincidir: esta opción le permite introducir el número de tipos de ICMP que desea filtrar.

Paso 14. El campo *ICMP Code* se habilita solamente cuando elige ICMP del Paso 5. Los códigos ICMP se utilizan para proporcionar información más específica sobre los mensajes de control. Haga clic en una de las opciones disponibles:

·Cualquiera: puede ser cualquier valor que coincida con el mensaje de control.

·Definido por el usuario: introduzca el código ICMP que desea filtrar.

Paso 15. El campo *IGMP (Internet Group Management Protocol)* sólo se habilita cuando se elige IGMP del paso 5. IGMP administra la pertenencia de host en grupos de multidifusión IP en un segmento de red. Haga clic en uno de los botones de opción disponibles para filtrar tipos de mensajes IGMP:

·Cualquiera: esta opción acepta todos los tipos de mensajes IGMP.

·Seleccionar de la lista: elija una de las opciones disponibles en la lista desplegable para filtrar:

- DVMRP: utiliza una técnica de inundación de trayectoria inversa, que envía una copia de un paquete recibido a través de cada interfaz excepto la que recibió el paquete.

- Consulta de host: envía periódicamente mensajes generales de consulta de host en cada red conectada para obtener información

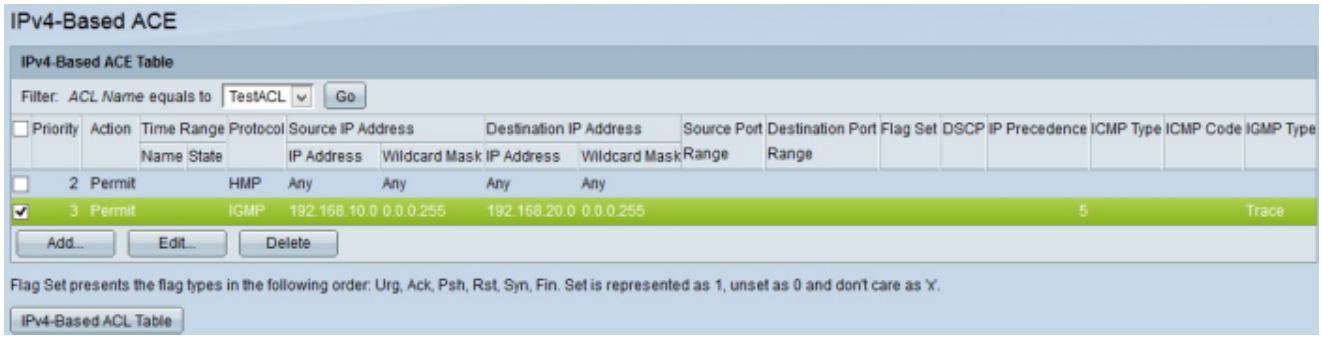
- Host-Reply — Responde a la consulta .

- PIM: se utiliza entre los routers multicast locales y remotos para dirigir el tráfico multicast desde el servidor multicast a muchos clientes multicast.

- Seguimiento: proporciona información para unirse y salir de un grupo de multidifusión IGMP.

·Tipo de coincidencia IGMP: esta opción permite introducir el número de tipos IGMP que desea filtrar.

Paso 16. Haga clic en **Apply** para guardar la configuración.



Paso 17. (Opcional) Para editar una regla de acceso actual, active la casilla de verificación de la regla de acceso que desea editar y haga clic en **Editar**.

Paso 18. (Opcional) Para eliminar una regla de acceso actual, active la casilla de verificación de la regla de acceso que desea eliminar y haga clic en **Eliminar**.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).