El MAC basó la lista de control de acceso (ACL) y la configuración de la Entrada de control de acceso (ACE) en el Switches manejado las 300 Series

Objetivo

Una lista de control de acceso (ACL) es una tecnología de seguridad que se utiliza al flujo del tráfico de la red del permit or deny. Información MAC basada de la capa 2 del uso ACL al acceso del permit or deny a traficar. Una Entrada de control de acceso (ACE) contiene los criterios reales de la regla de acceso. Una vez que se crea ACE, se aplica a un ACL. El Switches manejado las 300 Series soporta un máximo de 512 ACL y de 512 ACE.

Este artículo explica cómo crear los ACL basados MAC y cómo aplicar los ACE a los ACL en el Switches manejado las 300 Series.

Dispositivos aplicables

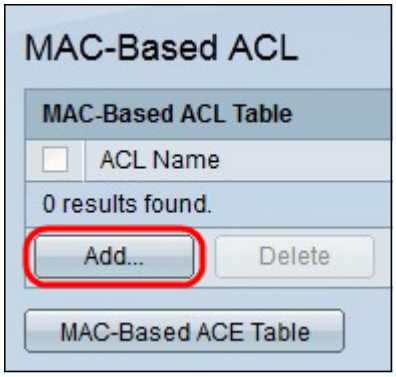
- SG300-10PP
- SG300-10MPP
- SG300-28PP-R
- SG300-28SFP-R
- SF302-08MPP
- SF302-08PP
- SF300-24PP-R
- SF300-48PP-R

Versión del software

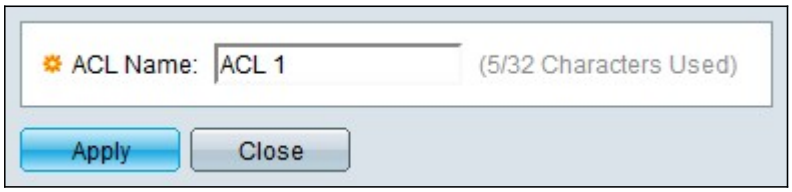
- 1.4.0.00p3 [SG300-28SFP-R]
- [All other Applicable Devices] de 6.2.10.18

ACL MAC basado

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija el **control de acceso > el ACL basado MAC**. La página *basada MAC ACL* se abre:

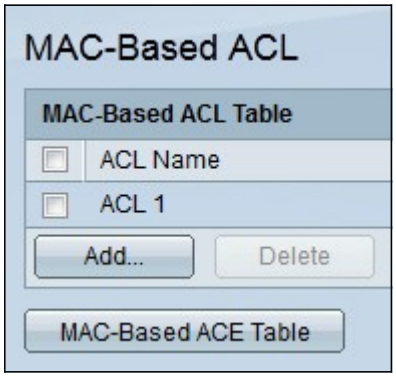


Paso 2. Haga click en Add La ventana *MAC basada del agregar ACL* aparece.



Paso 3. Ingrese un nombre para el ACL en el campo de nombre ACL.

Paso 4. El tecleo **se aplica**. Se crea El ACL.



ACE MAC basado

Cuando una trama se recibe en un puerto, el Switch procesa la trama con el primer ACL. Si la trama hace juego un filtro de ACE del primer ACL, la acción de ACE ocurre. Si la trama no hace juego ningunos de los filtros de ACE, se procesa el ACL siguiente. Si no se encuentra ninguna coincidencia a ningún ACE en todos los ACL relevantes, la trama se cae por abandono.

Nota: Esta acción predeterminada se puede evitar por la creación de una prioridad baja ACE que permita todo el tráfico.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija el **control de acceso > ACE basado MAC**. La página *basada MAC de ACE* se abre:

Paso 2. De la lista desplegable del nombre ACL, elija un ACL para aplicar una regla a.

Paso 3. El tecleo **va**. Se visualizan los ACE que se configuran ya para el ACL.

Paso 4. El tecleo **agrega** para agregar una nueva regla al ACL. La ventana *MAC basada de ACE del agregar* aparece.

El campo de nombre ACL visualiza el nombre del ACL.

Paso 5. Ingrese el valor de prioridad para el ACE en el campo de prioridad. Los ACE con un valor más prioritario se procesan primero. El valor 1 es la prioridad más alta.

Paso 6. Haga clic el botón de radio que corresponde a la acción deseada se toma que

cuando una trama cumple los criterios requeridos de ACE.

- Permiso — Del Switch los paquetes adelante que cumplen los criterios requeridos de ACE.
- Niegue — El Switch cae los paquetes que no cumplen los criterios requeridos de ACE.
- Apague — El Switch cae los paquetes que no cumplen los criterios requeridos del ACE y inhabilita el puerto en donde los paquetes fueron recibidos.

Nota: Los puertos discapacitados se pueden reactivar en la página de las *configuraciones de puerto*.

Paso 7. Marque la casilla de verificación del **permiso** en el campo del rango de tiempo para permitir que un rango de tiempo sea configurado a ACE. Los rangos de tiempo se utilizan para limitar la cantidad de tiempo que ACE está en efecto.

Paso 8. De la lista desplegable del nombre del rango de tiempo, elija un rango de tiempo para aplicarse a ACE.

Nota: Haga clic **editan** para navegar a y para crear un rango de tiempo en la página del *rango de tiempo*.

Paso 9. Haga clic el botón de radio que corresponde a los criterios deseados de ACE en el campo de la dirección MAC del destino.

- Ningunos — Todos los direccionamientos del MAC de destino se aplican a ACE.
- Definido por el usario — Ingrese un MAC address y a la máscara comodín MAC que debe ser aplicada al ACE en los campos del valor del MAC address del destino y de la máscara comodín del MAC de destino. Utilizan a las máscaras comodín para definir un rango de las direcciones MAC.

Paso 10. Haga clic el botón de radio que corresponde a los criterios deseados de ACE en el campo de MAC Address de origen.

- Ningunos — Todos los MAC Address de origen se aplican a ACE.
- Definido por el usario — Ingrese un MAC address y a la máscara comodín MAC que debe ser aplicada al ACE en los campos del valor del MAC address del destino y de la máscara comodín del MAC de destino. Utilizan a las máscaras comodín para definir un rango de las direcciones MAC.

Paso 11 Ingrese un VLAN ID que sea correspondido con con la etiqueta del VLA N del bastidor.

Paso 12. (Opcional) para incluir los valores 802.1p en los criterios de ACE, el control **incluye** en el campo 802.1p. 802.1p implica el Clase de Servicio (CoS) de la tecnología. CoS es un campo de bit 3 en una trama Ethernet que se utilice para distinguir el tráfico.

Paso 13. Si los valores 802.1p son incluidos, ingrese los campos siguientes.

- valor 802.1p — Ingrese el valor 802.1p que debe ser correspondido con. 802.1p es una especificación que da a 2 Switch de la capa la capacidad de dar prioridad al tráfico y de realizar el filtrado de multidifusión dinámico.

- máscara 802.1p — Ingrese a la máscara comodín de los valores 802.1p. Utilizan a esta máscara comodín para definir el rango de los valores 802.1p.

Paso 14. Ingrese el Ethertype del bastidor que debe ser correspondido con. El Ethertype es un campo de dos octetos en una trama Ethernet que se utilice para indicar qué protocolo se utiliza para el payload del bastidor.

Paso 15. Haga clic en Apply (Aplicar). Se crea ACE. En este ejemplo, ACE creado niega el tráfico que se envía de los MAC Address de origen definidos a todas las direcciones destino.