

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

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 lista de control de acceso (ACL) basada en el control de acceso a medios (MAC) es una lista de direcciones MAC de origen que utilizan información de capa 2 para permitir o denegar el acceso al tráfico. Si un paquete proviene de un punto de acceso inalámbrico a un puerto de red de área local (LAN) o viceversa, este dispositivo comprobará si la dirección MAC de origen del paquete coincide con cualquier entrada de esta lista y verifica las reglas ACL en relación con el contenido de la trama. Luego utiliza los resultados coincidentes para permitir o denegar este paquete. Sin embargo, los paquetes de LAN a puerto LAN no se verificarán. Una entrada de control de acceso (ACE) contiene los criterios de regla de acceso reales. Una vez que se crea la ACE, se aplica a una ACL. 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.

En este artículo se proporcionan instrucciones sobre cómo configurar ACL y ACE basadas en MAC en su switch administrado.

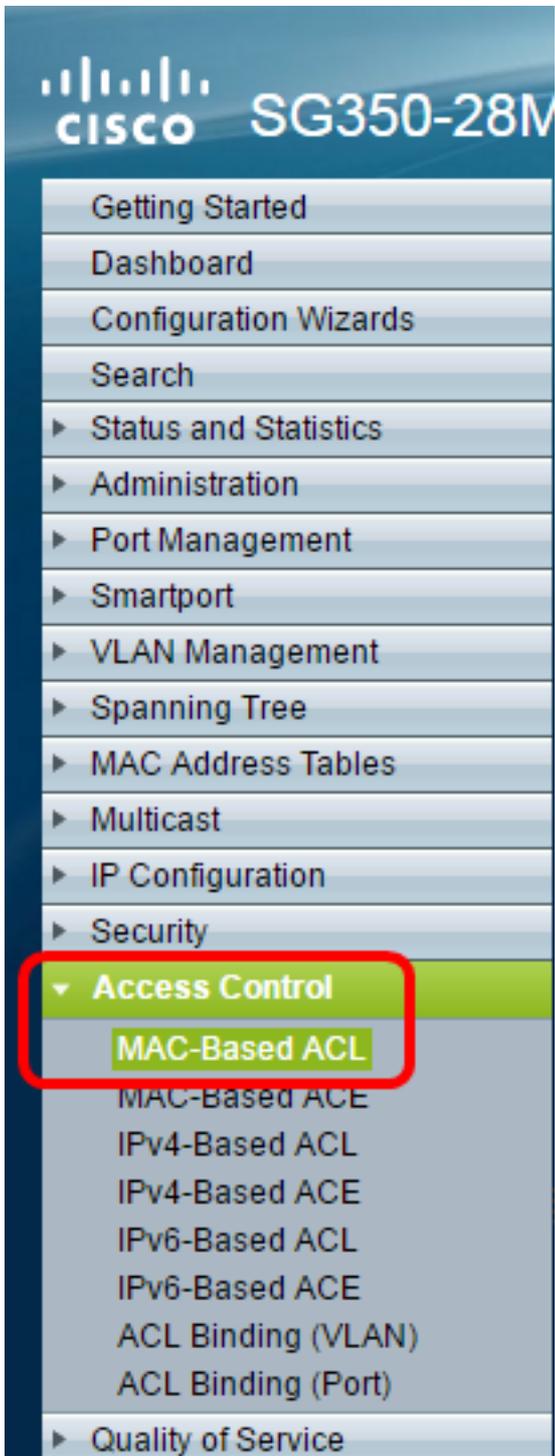
Dispositivos aplicables | Versión de software

- Serie Sx350 | 2.2.0.66 ([Descarga más reciente](#))
- Serie SG350X | 2.2.0.66 ([Descarga más reciente](#))
- Serie Sx500 | 1.4.5.02 ([última descarga](#))
- Serie Sx550X | 2.2.0.66 ([Descarga más reciente](#))

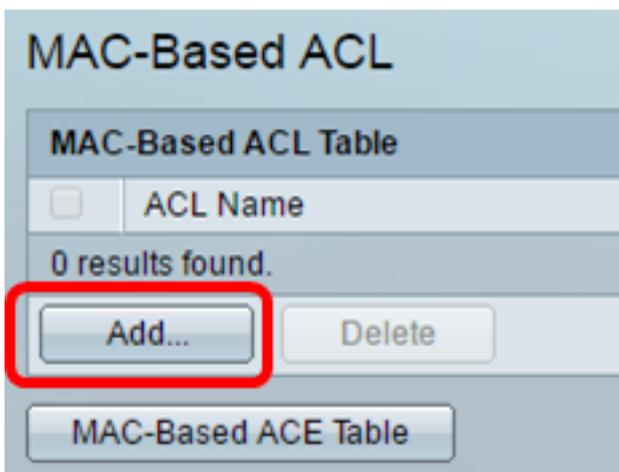
Configuración de ACL y ACE basadas en MAC

Configuración de ACL Basada en MAC

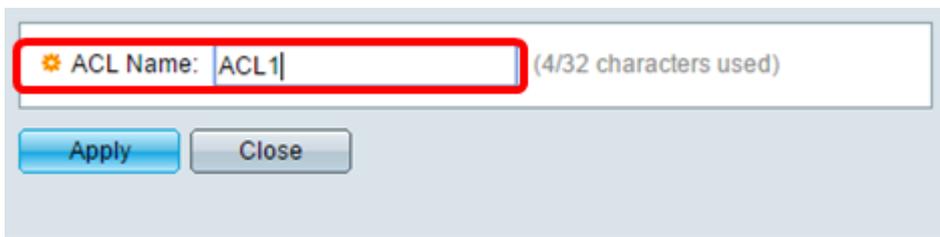
Paso 1. Inicie sesión en la utilidad basada en Web y luego vaya a **Control de Acceso > ACL Basada en MAC**.



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



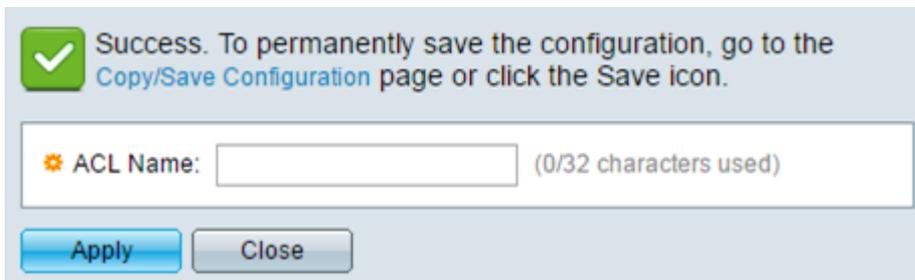
Paso 3. Introduzca el nombre de la nueva ACL en el campo Nombre de ACL.



ACL Name: ACL1 (4/32 characters used)

Apply Close

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

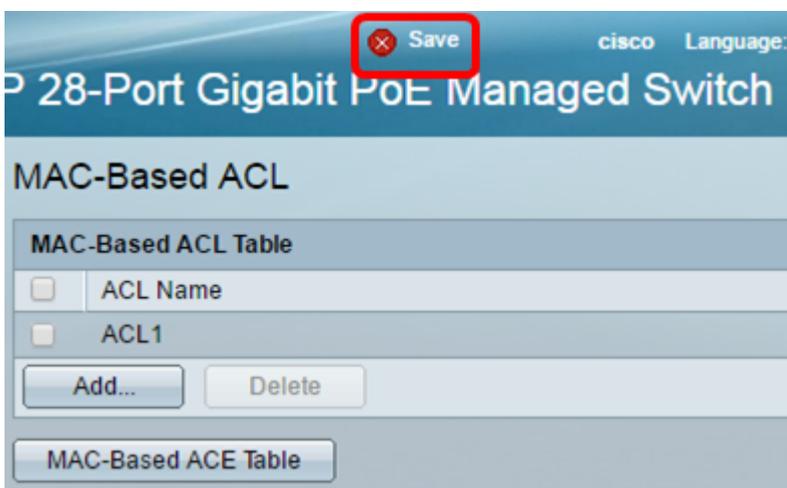


Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

ACL Name: (0/32 characters used)

Apply Close

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



Save cisco Language:

28-Port Gigabit PoE Managed Switch

MAC-Based ACL

MAC-Based ACL Table

ACL Name

ACL1

Add... Delete

MAC-Based ACE Table

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

Configuración de ACE basada en MAC

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

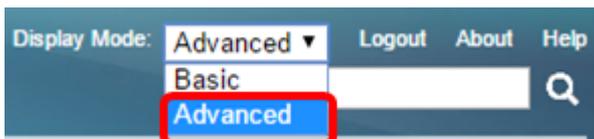
En este escenario, se creará una ACE para denegar el tráfico que se envía desde una dirección MAC de origen definida por el usuario específica a cualquier dirección de destino.

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

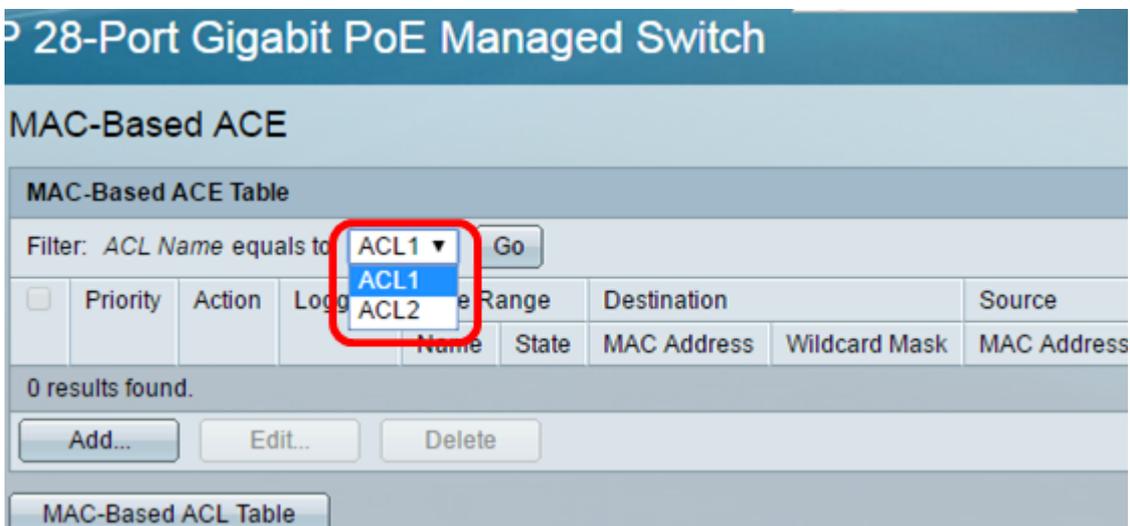
Paso 1. En la utilidad basada en web, vaya a **Access Control > MAC-Based ACE**.



Importante: Para utilizar completamente las funciones y características disponibles del switch, cambie al modo avanzado seleccionando **Avanzado** en la lista desplegable Modo de visualización 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.

ACL Name:	ACL1
<input checked="" type="checkbox"/> Priority:	<input type="text" value="1"/> (Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Logging:	<input checked="" type="checkbox"/> Enable

Paso 5. (Opcional) Marque la casilla de verificación Activar registro para habilitar los flujos ACL de registro que coincidan con la regla ACL.

Paso 6. 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 Denegar.

<input checked="" type="checkbox"/> Priority:	<input type="text" value="1"/> (Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown

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.

Nota: Los puertos desactivados se pueden reactivar en la página Port Settings (Configuración de puerto).

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.

Time Range:	<input checked="" type="checkbox"/> Enable
Time Range Name:	<input type="text" value="1"/> Edit

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

Time Range:	<input checked="" type="checkbox"/> Enable
Time Range Name:	<input type="text" value="1"/> Edit

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

Time Range Name: 1 (1/32 characters used)

Absolute Starting Time: Immediate
 Date 2016 Jan 01 Time 00 00 HH:MM

Absolute Ending Time: Infinite
 Date 2017 Dec 01 Time 23 59 HH:MM

Apply Close

Paso 9. Haga clic en el botón de opción que se corresponda con los criterios deseados de ACE en el área Destination MAC Address (Dirección MAC de destino).

Destination MAC Address: Any
 User Defined

* Destination MAC Address Value:

* Destination MAC Wildcard Mask: (0s for matching, 1s for no matching)

Las opciones son:

Any: todas las direcciones MAC de destino se aplican a ACE.

Definido por el Usuario: introduzca una dirección MAC y una máscara comodín MAC que se aplicarán a ACE en los campos *Valor de dirección MAC de destino* y *Máscara comodín MAC de destino*. Las máscaras comodín se utilizan para definir un rango de direcciones MAC.

Nota: En este ejemplo, se elige Any (Cualquiera). Si elige esta opción, la ACE que se creará denegará el tráfico ACE.

Paso 10. Haga clic en el botón de opción que se corresponda con los criterios deseados de ACE en el área Dirección MAC de Origen.

ACL Name:	ACL1	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="1"/> Edit	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
* Destination MAC Address Value:	<input type="text"/>	
* Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Source MAC Address Value:	<input type="text" value="a2:b2:c2:d2:e2:f2"/>	
Source MAC Wildcard Mask:	<input type="text" value="000000001111"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text" value="2"/>	(Range: 1 - 4094)
802.1p:	<input checked="" type="checkbox"/> Include	
802.1p Value:	<input type="text" value="1"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text" value="0"/>	(Range: 0 - 7)
Ethertype:	<input type="text" value="88AB"/>	(Range: 5DD - FFFF)
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

Las opciones son:

Any: todas las direcciones MAC de origen se aplican a ACE.

Definido por el Usuario: introduzca una dirección MAC y una máscara comodín MAC que se aplicarán a la ACE en los *campos Source MAC Address Value* y *Source MAC Wildcard Mask*. Las máscaras comodín se utilizan para definir un rango de direcciones MAC.

Nota: En este ejemplo, se elige Definido por el usuario.

Paso 11. (Opcional) En el campo *VLAN ID*, ingrese un ID de VLAN que coincidirá con la etiqueta VLAN de la trama.

Paso 12. (Opcional) Para incluir valores 802.1p en los Criterios ACE, marque **Incluir** en la casilla de verificación 802.1p. 802.1p incluye la clase de servicio (CoS) de tecnología. CoS es un campo de 3 bits en una trama Ethernet que se utiliza para diferenciar el tráfico.

Paso 13. Si se incluyen los valores de 802.1p, introduzca los campos siguientes:

Valor 802.1p: introduzca el valor 802.1p que se debe igualar. 802.1p es una especificación

que proporciona a los switches de Capa 2 la capacidad de priorizar el tráfico y realizar un filtrado de multidifusión dinámico. Los valores son los siguientes:

- 0 — Antecedentes. Los datos que tienen menos prioridad, como las transferencias masivas, los juegos, etc.
- 1: el mejor esfuerzo. Los datos que necesitan entrega con el mejor esfuerzo en prioridad LAN normal. La red no proporciona ninguna garantía sobre la entrega, pero los datos obtienen una velocidad de bits sin especificar y un tiempo de entrega basado en el tráfico.
- 2: Excelente esfuerzo. Los datos que requieren el mejor esfuerzo para los usuarios importantes.
- 3: aplicación crítica como el protocolo de inicio de sesión (SIP) del teléfono de Linux Virtual Server (LVS).
- 4 — Vídeo. Latencia y fluctuación inferiores a 100 ms.
- 5: Voz predeterminada del teléfono IP de Cisco. Latencia y fluctuación inferiores a 10 ms.
- 6: protocolo de transporte en tiempo real (RTP) del teléfono LVS de control de red.
- 7: Control de red. Alto requisito para poder mantener y admitir la infraestructura de red.

Máscara 802.1p: introduzca la máscara comodín de los valores 802.1p. Esta máscara comodín se utiliza para definir el rango de valores 802.1p.

Paso 14. (Opcional) Introduzca el tipo Ethertype de la trama que se va a hacer coincidir. Ethertype es un campo de 2 octetos en una trama Ethernet que se utiliza para indicar qué protocolo se utiliza para la carga útil de la trama.

Paso 14. Haga clic en **Aplicar** y luego haga clic en **Cerrar**. La ACE se crea y se asocia al nombre de la ACL.

Paso 15. Haga clic en **Guardar** para guardar la configuración en el archivo de configuración de inicio.

28-Port Gigabit PoE Managed Switch

MAC-Based ACE

MAC-Based ACE Table

Filter: ACL Name equals to

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Destination
				Name	State	MAC Address
<input type="checkbox"/>	1	Deny	Enabled	1	Active	Any
<input type="checkbox"/>	2	Permit	Enabled	1	Active	a1:b1:c1:d1:e1:f1

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

Otros enlaces que puede encontrar valiosos:

- [Página de productos de switches de la serie 350](#)
- [Página de productos de switches serie 350X](#)
- [Página de producto de switches de la serie 550](#)
- [Página de productos de switches de la serie 550X](#)

Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)