Configurar a ACL (Access Control List, lista de controle de acesso) baseada em MAC e a entrada de controle de acesso (ACE) em um switch gerenciado

Objetivo

Uma lista de controle de acesso (ACL) é uma lista de filtros de tráfego de rede e ações correlacionadas usadas para melhorar a segurança. Bloqueia ou permite que os usuários acessem recursos específicos. Uma ACL contém os hosts com permissão ou negação de acesso ao dispositivo de rede. A ACL (Media Access Control) baseada no Controle de Acesso ao Meio (MAC - Media Access Control List) é uma lista de endereços MAC de origem que usam informações da Camada 2 para permitir ou negar acesso ao tráfego. Se um pacote estiver vindo de um ponto de acesso sem fio para uma porta LAN (Local Area Network, rede local) ou vice-versa, esse dispositivo verificará se o endereço MAC origem do pacote corresponde a qualquer entrada nessa lista e verificará as regras da ACL em relação ao conteúdo do quadro. Em seguida, ele usa os resultados correspondentes para permitir ou negar esse pacote. No entanto, os pacotes da porta LAN para a porta LAN não serão verificados. Uma entrada de controle de acesso (ACE) contém os critérios reais da regra de acesso. Quando a ACE é criada, ela é aplicada a uma ACL. Você deve usar listas de acesso para fornecer um nível básico de segurança para acessar sua rede. Se você não configurar listas de acesso em seus dispositivos de rede, todos os pacotes que passam pelo switch ou roteador poderão ser permitidos em todas as partes da rede.

Este artigo fornece instruções sobre como configurar a ACL baseada em MAC e a ACE no seu Switch Gerenciado.

Dispositivos aplicáveis | Versão do software

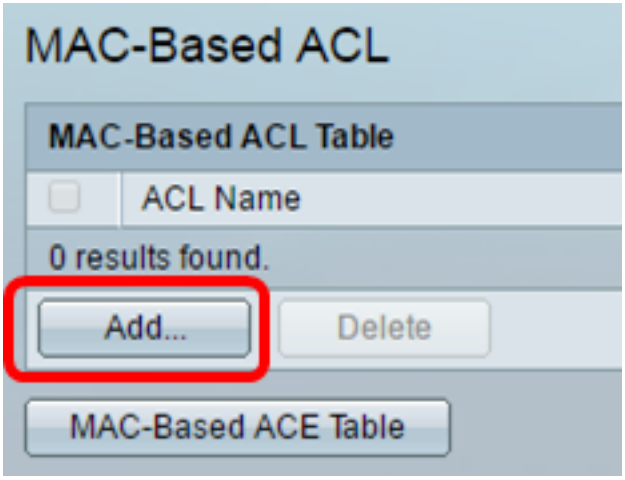
- Sx350 Series | 2.2.0.66 (Baixe o mais recente)
- SG350X Series | 2.2.0.66 (Baixe o mais recente)
- Sx500 Series | 1.4.5.02 (Baixe o mais recente)
- Sx550X Series | 2.2.0.66 (Baixe o mais recente)

Configurar ACL baseada em MAC e ACE

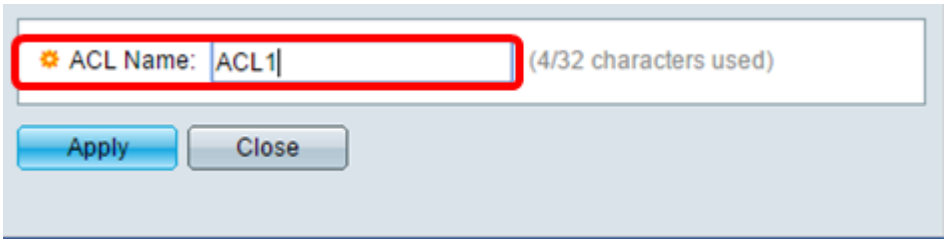
Configurar ACL baseada em MAC

Etapa 1. Faça login no utilitário baseado na Web e vá para **Controle de acesso > ACL baseada em MAC**.

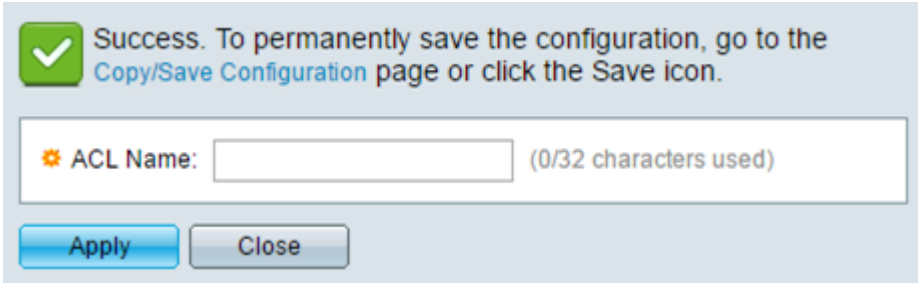
Etapa 2. Clique no botão Adicionar.



Etapa 3. Digite o nome da nova ACL no campo Nome da ACL.



Etapa 4. Clique em **Aplicar** e, em seguida, clique em **Fechar**.



Etapa 5. (Opcional) Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.

Agora você deve ter configurado uma ACL com base em MAC em seu switch.

Configurar ACE baseada em MAC

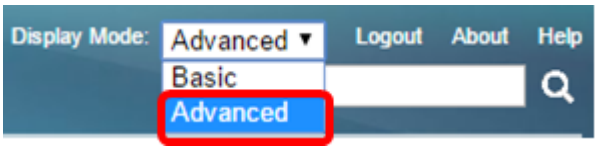
Quando um quadro é recebido em uma porta, o switch processa o quadro através da primeira ACL. Se o quadro corresponder a um filtro ACE da primeira ACL, a ação ACE ocorrerá. Se o quadro não corresponder a nenhum dos filtros ACE, a próxima ACL será processada. Se não for encontrada nenhuma correspondência para qualquer ACE em todas as ACLs relevantes, o quadro será descartado por padrão.

Nesse cenário, uma ACE será criada para negar o tráfego enviado de um endereço MAC de origem definido pelo usuário específico para qualquer endereço de destino.

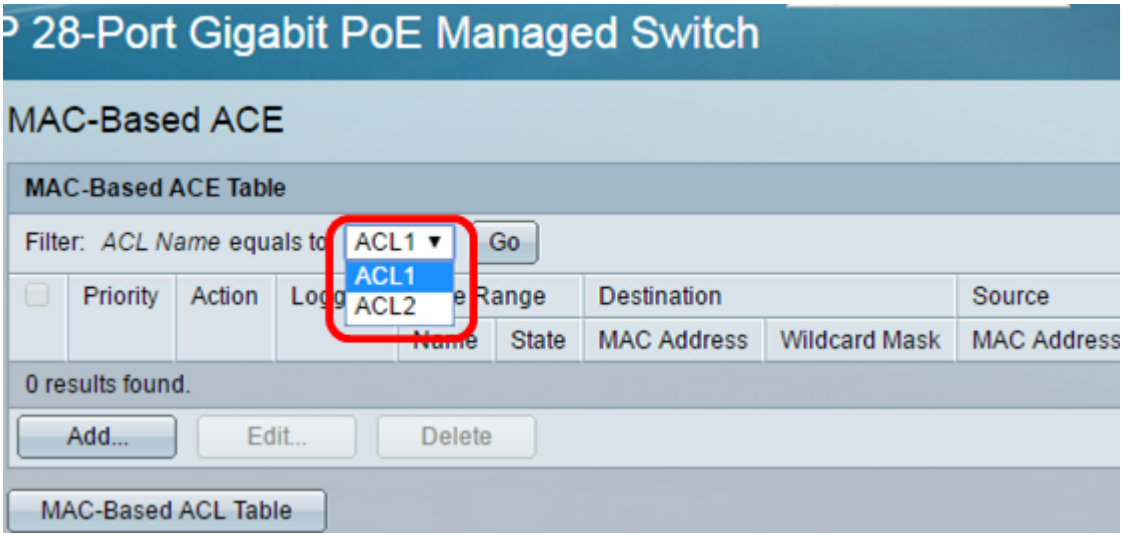
Note: Essa ação padrão pode ser evitada pela criação de uma ACE de baixa prioridade que permita todo o tráfego.

Etapa 1. No utilitário baseado na Web, vá para **Controle de acesso > ACE baseada em MAC**.

Importante: Para utilizar plenamente os recursos e as funções disponíveis do switch, altere para o modo Avançado escolhendo **Avançado** na lista suspensa Modo de exibição no canto superior direito da página.



Etapa 2. Escolha uma ACL na lista suspensa Nome da ACL e clique em **Ir**.

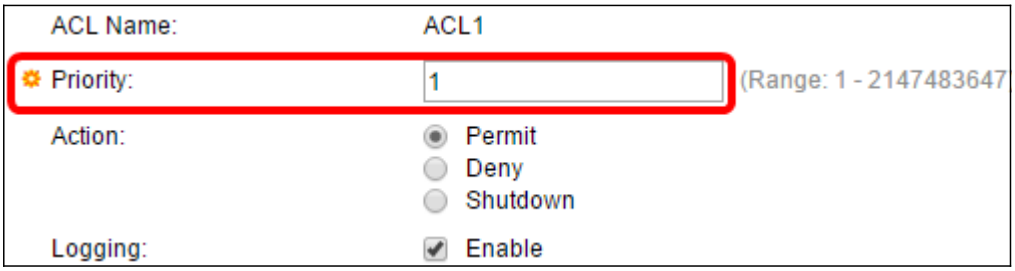


Note: As ACEs já configuradas para a ACL serão exibidas na tabela.

Etapa 3. Clique no botão **Add** para adicionar uma nova regra à ACL.

Note: O campo *ACL Name* exibe o nome da ACL.

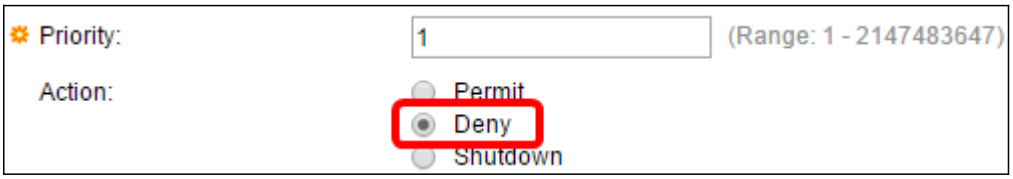
Etapa 4. Insira o valor de prioridade para a ACE no campo *Prioridade*. As ACEs com um valor de prioridade mais alto são processadas primeiro. O valor 1 é a prioridade mais alta.



Etapa 5. (Opcional) Marque a caixa de seleção Ativar registro para ativar os fluxos de registro da ACL que correspondem à regra da ACL.

Etapa 6. Clique no botão de opção que corresponde à ação desejada que é tomada quando um quadro atende aos critérios exigidos da ACE.

Note: Neste exemplo, Negar é escolhido.



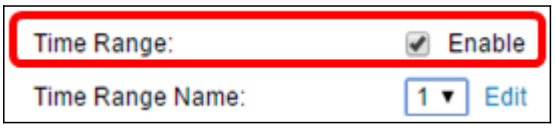
Permit (Permitir) — O switch encaminha pacotes que atendem aos critérios exigidos da ACE.

Negar — O switch descarta pacotes que atendem aos critérios exigidos da ACE.

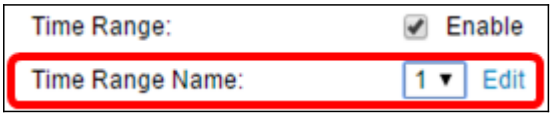
Desligamento — O switch descarta pacotes que não atendem aos critérios exigidos da ACE e desativa a porta onde os pacotes foram recebidos.

Note: As portas desativadas podem ser reativadas na página Configurações de porta.

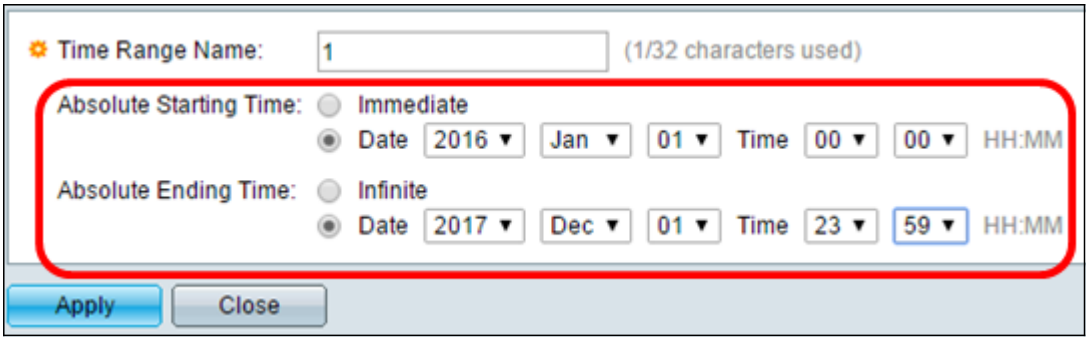
Passo 7. (Opcional) Marque a caixa de seleção **Habilitar** intervalo de tempo para permitir que um intervalo de tempo seja configurado para a ACE. Os intervalos de tempo são usados para limitar o tempo durante o qual uma ECA está em vigor.



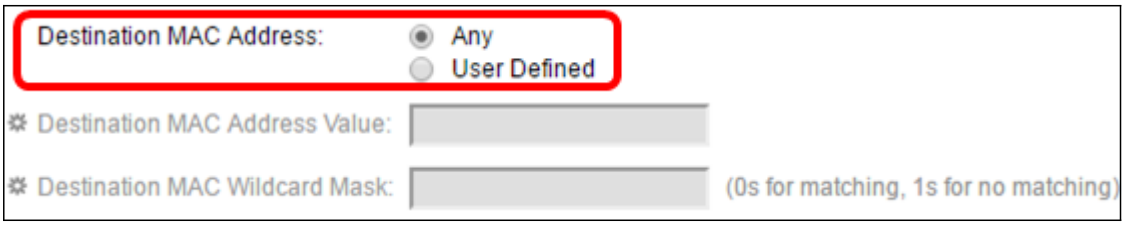
Etapa 8. (Opcional) Na lista suspensa Nome do intervalo de tempo, escolha um intervalo de tempo para aplicar à ACE.



Note: Você pode clicar em **Editar** para navegar até e criar um intervalo de tempo na página Intervalo de tempo.



Etapa 9. Clique no botão de opção que corresponde aos critérios desejados da ACE na área Destination MAC Address (Endereço MAC de destino).



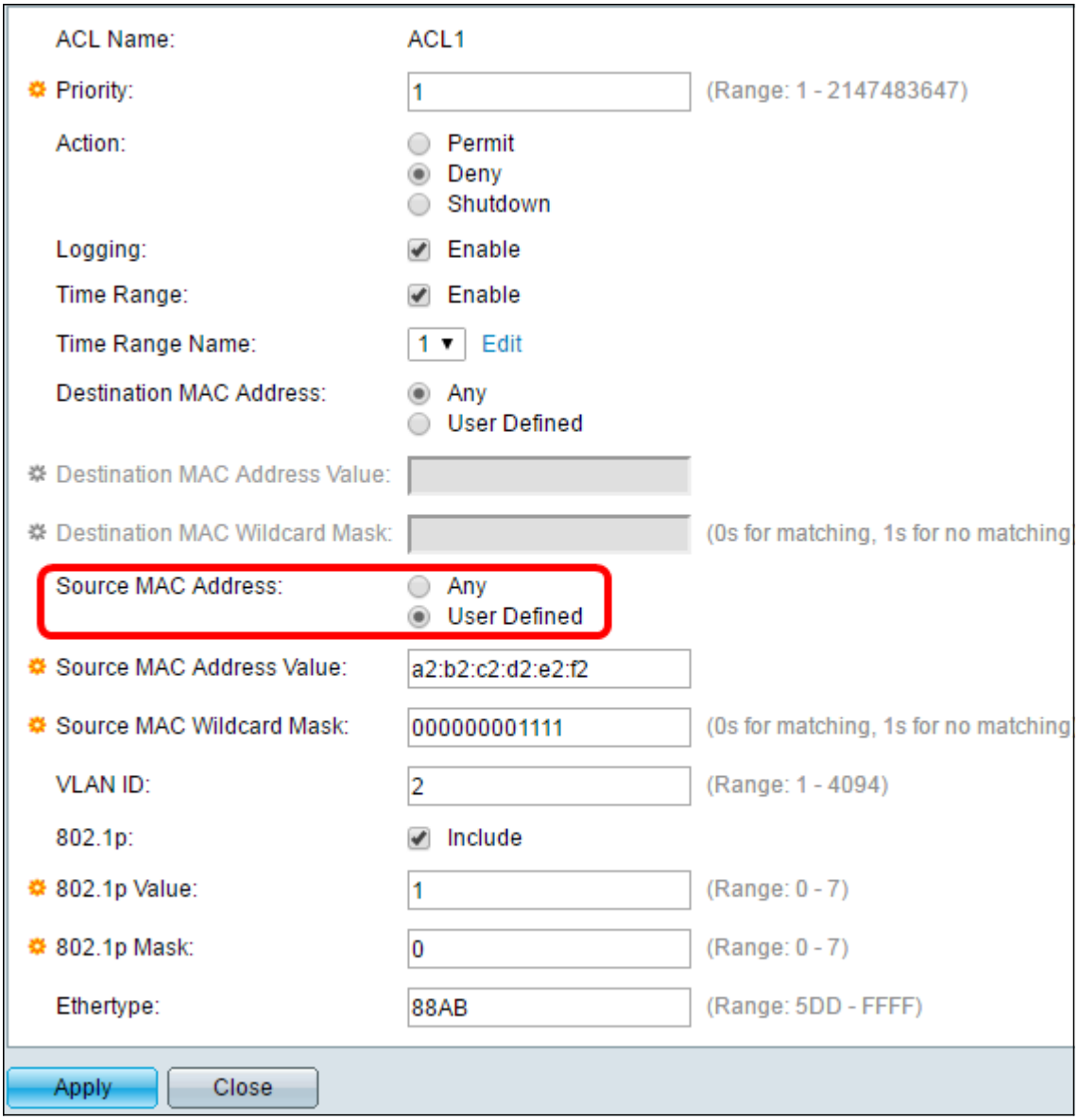
As opções são:

Qualquer - Todos os endereços MAC de destino se aplicam à ACE.

Definido pelo Usuário — Insira um endereço MAC e uma máscara curinga MAC a serem aplicados à ACE nos campos *Valor do Endereço MAC de Destino* e *Máscara Curinga de Destino MAC*. As máscaras curinga são usadas para definir um intervalo de endereços MAC.

Note: Neste exemplo, Qualquer é escolhido. Escolher essa opção significa que a ACE a ser criada negará o tráfego da ACE.

Etapa 10. Clique no botão de opção que corresponde aos critérios desejados da ACE na área Endereço MAC de Origem.



As opções são:

Qualquer - Todos os endereços MAC de origem se aplicam à ACE.

Definido pelo Usuário — Insira um endereço MAC e uma máscara curinga MAC a serem aplicados à ACE nos campos *Source MAC Address Value* e *Source MAC Wildcard Mask*. As máscaras curinga são usadas para definir um intervalo de endereços MAC.

Note: Neste exemplo, Definido pelo usuário é escolhido.

Etapa 11. (Opcional) No campo *VLAN ID*, insira uma VLAN ID que será correspondida com a marca VLAN do quadro.

Etapa 12. (Opcional) Para incluir valores 802.1p em Critérios de ACE, marque a caixa de seleção **Incluir** no 802.1p. O 802.1p envolve a Classe de Serviço de Tecnologia (CoS - Technology Class of Service). CoS é um campo de 3 bits em um quadro Ethernet usado para diferenciar o tráfego.

Etapa 13. Se os valores 802.1p forem incluídos, insira os seguintes campos:

Valor 802.1p — Insira o valor 802.1p a ser correspondido. O 802.1p é uma especificação que

dá aos switches da Camada 2 a capacidade de priorizar o tráfego e executar a filtragem multicast dinâmica. Os valores são os seguintes:

- 0 — Antecedentes. Os dados que são menos priorizados como transferências em massa, jogos e assim por diante.

- 1 — Melhor esforço. Os dados que precisam de entrega de melhor esforço em uma prioridade de LAN comum. A rede não oferece nenhuma garantia na entrega, mas os dados obtêm taxa de bits e tempo de entrega não especificados com base no tráfego.

- 2 — Excelente esforço. Os dados que precisam de entrega de melhor esforço para usuários importantes.

- 3 — Aplicativo Crítico, como o protocolo de inicialização de sessão telefônica (SIP) do servidor virtual Linux (LVS).

- 4 — Vídeo. Latência e instabilidade inferiores a 100 ms.

- 5 — Telefone IP de voz da Cisco padrão. Latência e instabilidade inferiores a 10 ms.

- 6 — Network Control LVS phone Real-time Transport Protocol (RTP).

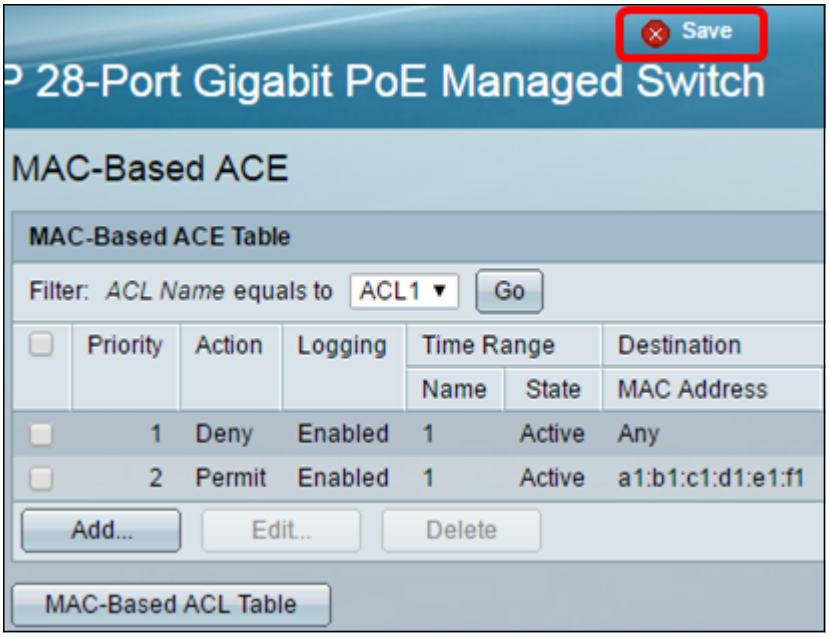
- 7 — Controlo da Rede. Alto requisito para manter e suportar a infraestrutura de rede.

Máscara 802.1p — Insira a máscara curinga dos valores 802.1p. Essa máscara curinga é usada para definir o intervalo de valores 802.1p.

Etapa 14. (Opcional) Insira o Ethertype do quadro a ser correspondido. Ethertype é um campo de 2 octetos em um quadro Ethernet usado para indicar qual protocolo é utilizado para a carga útil do quadro.

Etapa 14. Clique em **Aplicar** e, em seguida, clique em **Fechar**. A ACE é criada e associada ao nome da ACL.

Etapa 15. Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.



Agora você deve ter configurado uma ACE baseada em MAC em seu switch.

Outros links que você pode achar importantes:

- Página de produto dos switches 350 Series
- Página de produto dos switches 350X Series
- Página de produto dos switches 550 Series
- Página de produto dos switches 550X Series

Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco