Configurar a ACL (Access Control List, lista de controle de acesso) baseada em IPv6 e a entrada de controle de acesso (ACE) em um switch

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 funcionalidade típica da ACL no IPv6 é semelhante às ACLs no IPv4. As ACLs determinam qual tráfego bloquear e qual tráfego encaminhar nas interfaces do switch. As ACLs permitem a filtragem com base nos endereços de origem e de destino, de entrada e de saída para interfaces específicas. Cada ACL tem uma instrução deny implícita no final. As regras para as ACLs são configuradas nas entradas de controle de acesso (ACEs).

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 IPv6 e a ACE em um switch.

Dispositivos aplicáveis

- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

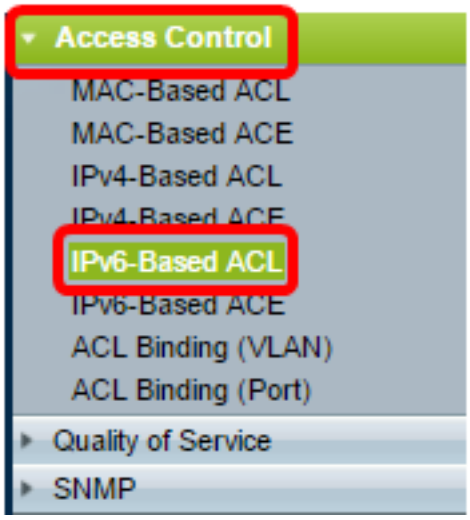
Versão de software

- 1.4.5.02 - Sx500 Series
- 2.2.5.68 - Sx350 Series, SG350X Series, Sx550X Series

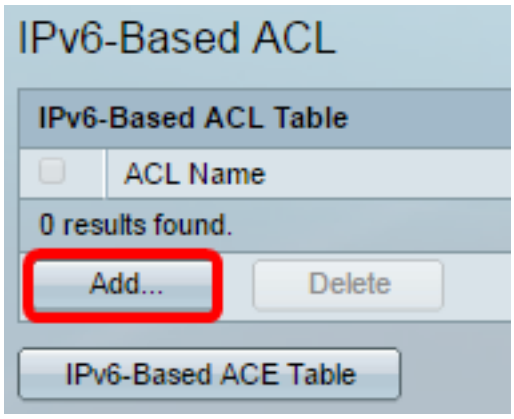
Configurar ACL baseada em IPv6 e ACE

Configurar ACL baseada em IPv6

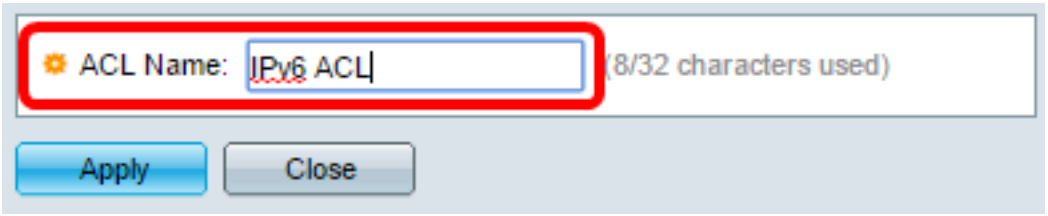
Etapa 1. Faça login no utilitário baseado na Web e vá para **Controle de acesso > ACL baseada em IPv6**.



Etapa 2. Clique no botão Adicionar.

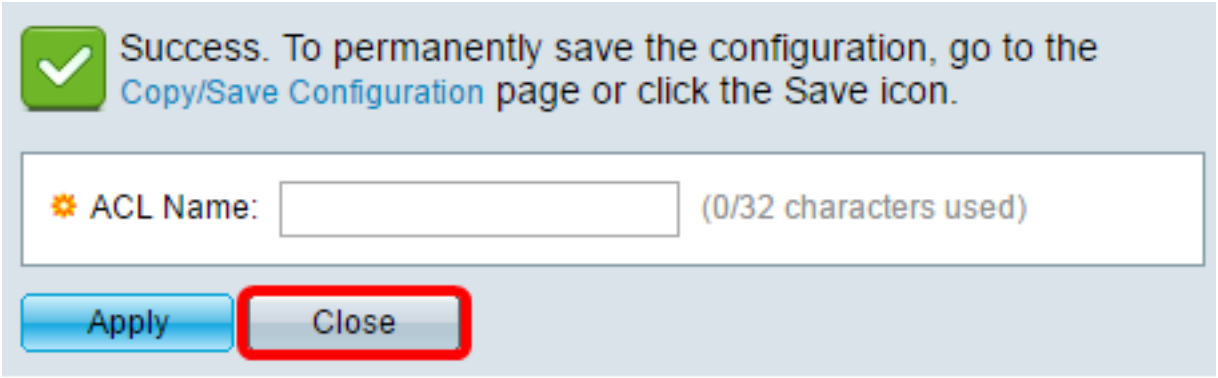


Etapa 3. Insira o nome da nova ACL no campo *ACL Name (Nome da ACL)*.



Note: Neste exemplo, a ACL IPv6 é usada.

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 baseada em IPv6 no switch.

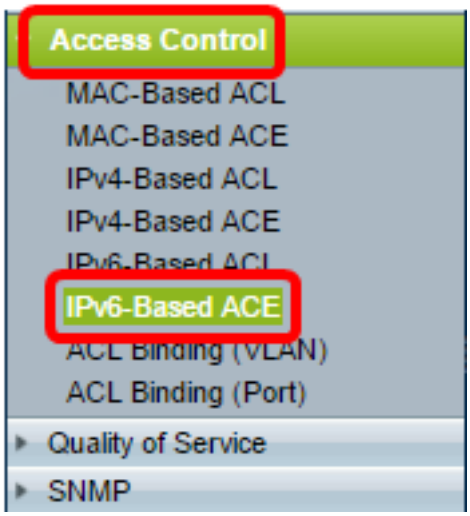
Configurar ACE baseada em IPv6

Quando um pacote é recebido em uma porta, o switch processa o quadro através da primeira ACL. Se o pacote corresponder a um filtro ACE da primeira ACL, a ação ACE ocorrerá. Se o pacote 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 pacote será descartado por padrão.

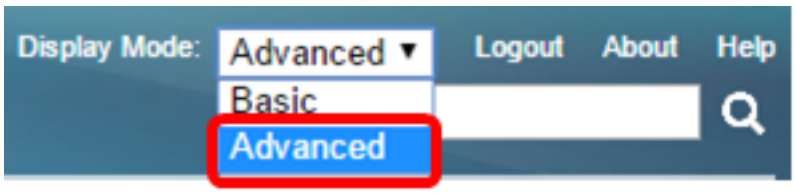
Nesse cenário, uma ACE será criada para negar o tráfego enviado de um endereço IPv6 de origem definido pelo usuário para qualquer endereço de destino.

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

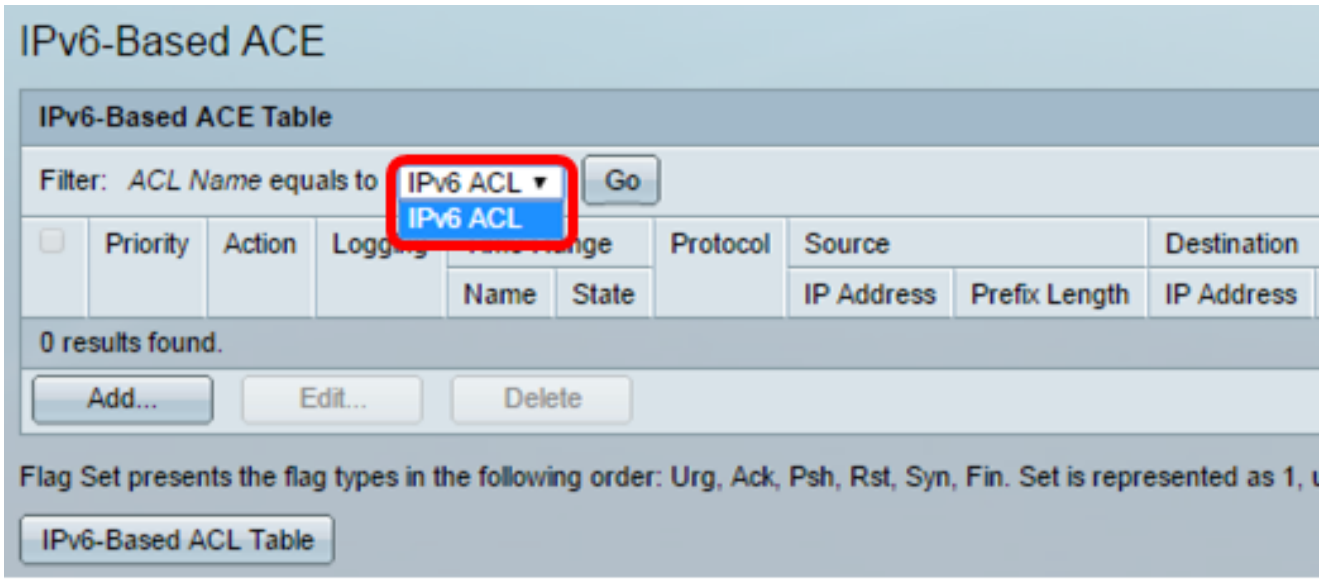
Etapa 1. No utilitário baseado na Web, vá para **Controle de acesso > ACE baseada em IPv6** .



Importante: Se você tiver um switch Sx350, SG350X, Sx550X, altere para o modo Avançado escolhendo **Avançado** na lista suspensa Modo de exibição no canto superior direito da página.

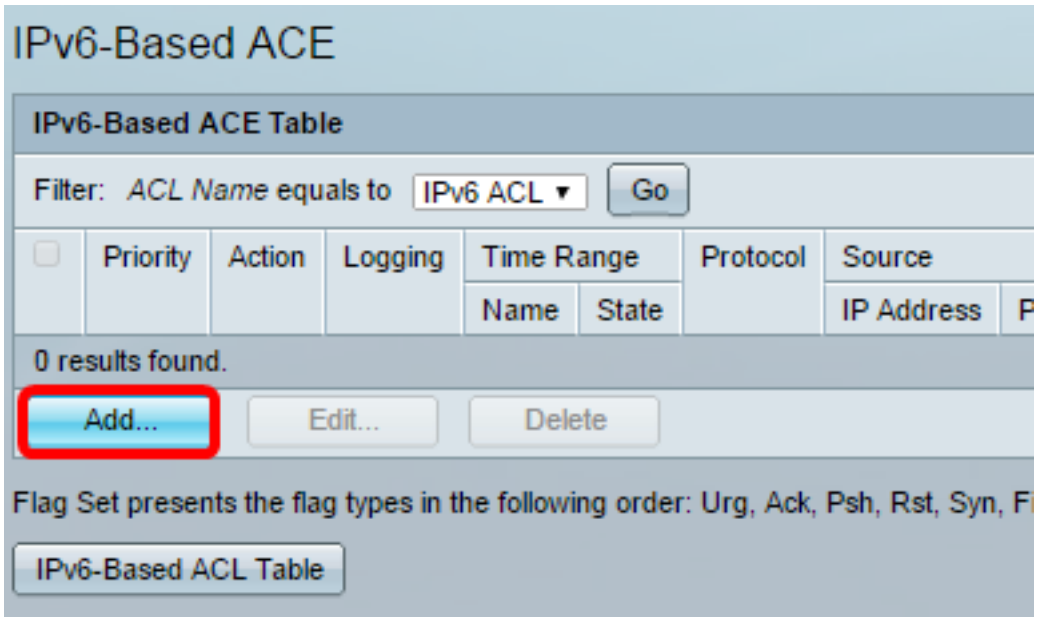


Etapa 2. Escolha uma ACL na lista suspensa Nome da ACL e clique em **Ir**.



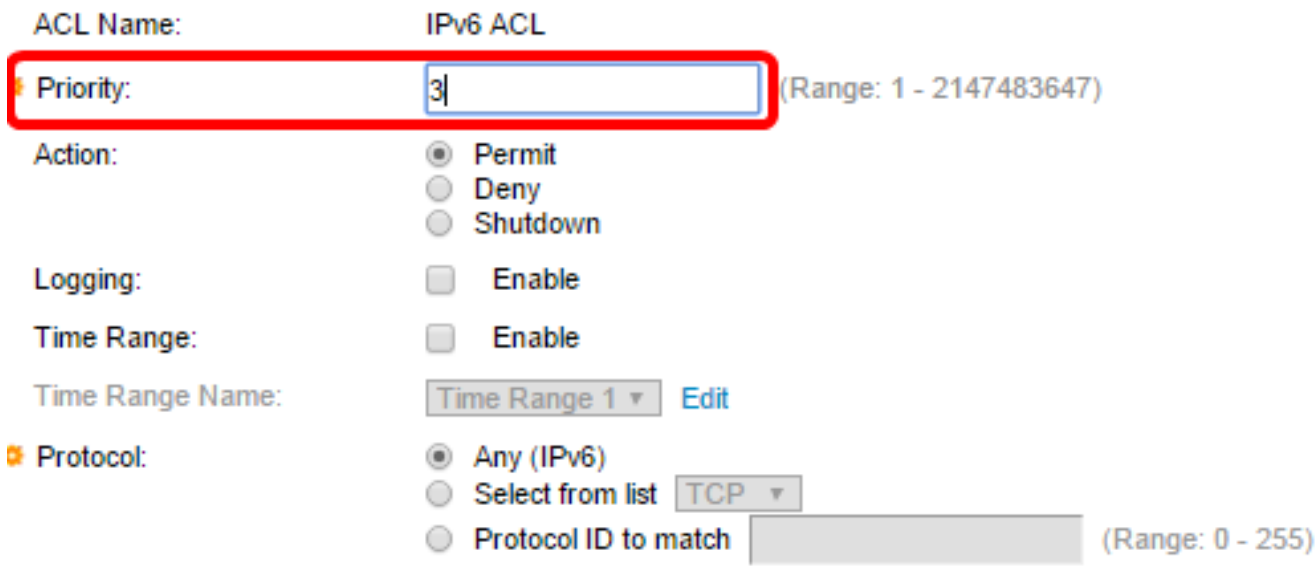
Note: As ACEs já configuradas para a ACL serão exibidas na tabela.

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. Tem um intervalo de 1 a 2147483647.



Note: Neste exemplo, 3 é usado.

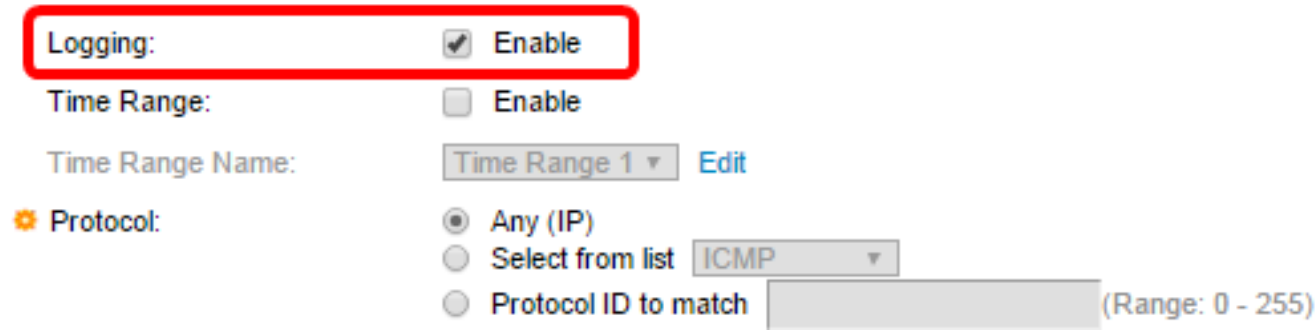
Etapa 5. Clique no botão de opção que corresponde à ação desejada que é tomada quando um quadro atende aos critérios exigidos da ACE.

Note: Neste exemplo, Permit é escolhido.

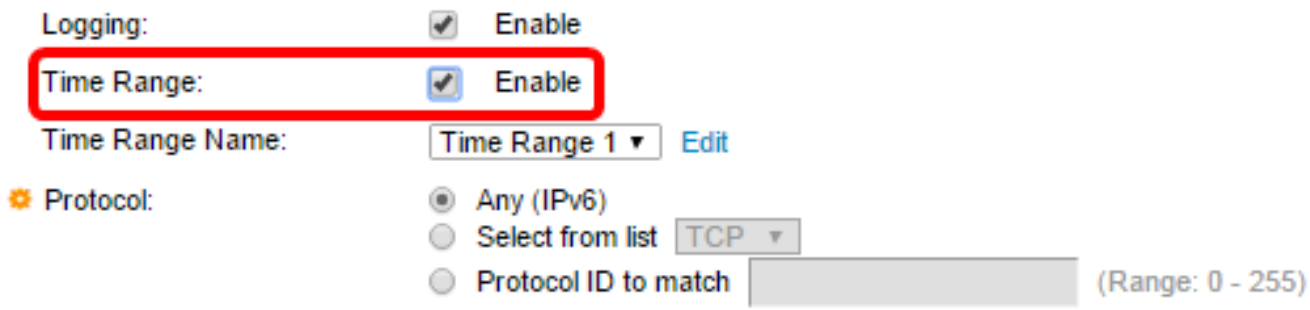
- Permit (Permitir) — O switch encaminha pacotes que atendem aos critérios exigidos da ACE.
- Negar — O switch descarta pacotes que atendem aos critérios exigidos da ACE.

Desligamento — O switch descarta pacotes que não atendem aos critérios exigidos da ACE e desativa a porta onde os pacotes foram recebidos. As portas desativadas podem ser reativadas na página Configurações de porta.

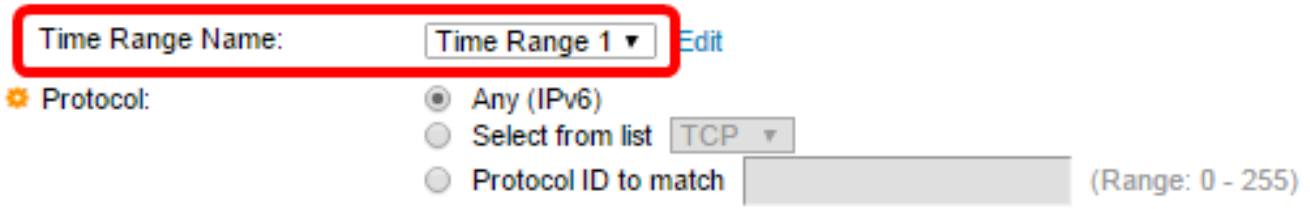
Etapa 6. (Opcional) Marque a caixa de seleção **Habilitar** registro para habilitar os fluxos de registro da ACL que correspondem à regra da ACL.



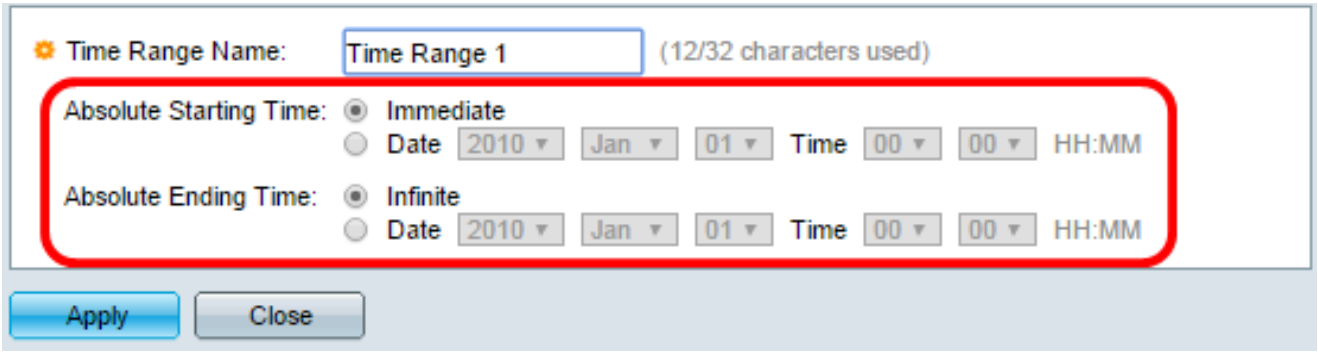
Passo 7. (Opcional) Marque a caixa de seleção **Habilitar** intervalo de tempo para permitir que um intervalo de tempo seja configurado para a ACE. Os intervalos de tempo são usados para limitar o tempo durante o qual uma ECA está em vigor. Se isso for deixado desabilitado, a ACE funcionará a qualquer momento.



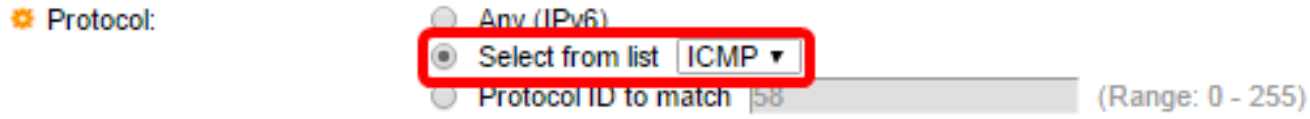
Etapa 8. (Opcional) Na lista suspensa Nome do intervalo de tempo, escolha um intervalo de tempo para aplicar à ACE.



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



Etapa 9. Escolha um tipo de protocolo na área Protocolo. A ACE será criada com base em um protocolo ou ID de protocolo específico.

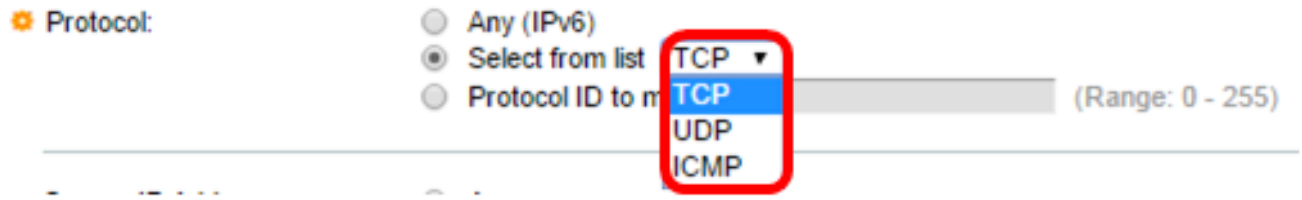


As opções são:

- Any (IP) — Essa opção configurará o ACE para aceitar todos os protocolos IP.
- Selecionar na lista — Essa opção permitirá que você escolha um protocolo em uma lista suspensa. Se preferir esta opção, vá para a Etapa 10.
- ID do protocolo correspondente — Essa opção permitirá que você digite uma ID do protocolo. Se preferir esta opção, vá para a Etapa 11.

Note: Neste exemplo, a opção Selecionar na lista é escolhida.

Etapa 10. (Opcional) Se você escolher Selecionar na lista na Etapa 9, escolha um protocolo na lista suspensa.

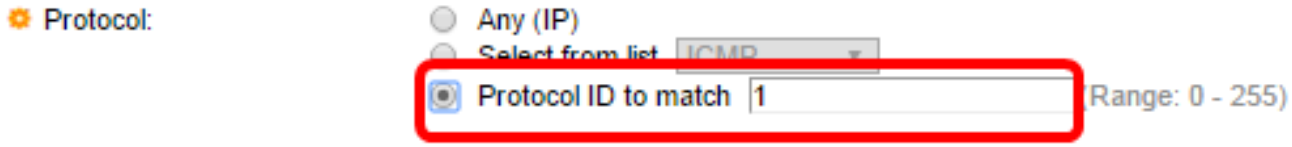


As opções são:

- TCP — O Transmission Control Protocol (TCP) permite que dois hosts se comuniquem e troquem fluxos de dados. O TCP garante a entrega de pacotes e garante que os pacotes sejam transmitidos e recebidos na ordem em que foram enviados.
- UDP — User Datagram Protocol (UDP) transmite pacotes, mas não garante sua entrega.
- ICMP — Corresponde pacotes ao Internet Control Message Protocol (ICMP).

Note: Neste exemplo, o TCP é usado.

Etapa 11. (Opcional) Se você escolheu a ID do protocolo para corresponder na Etapa 9, digite a ID do protocolo no *ID do protocolo para corresponder ao* campo.



Note: Neste exemplo, 1 é usado.

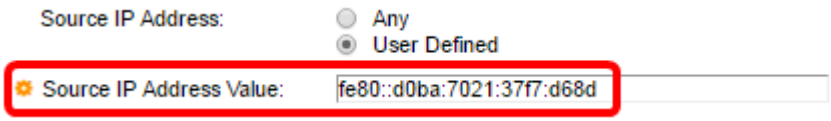
Etapa 12. Clique no botão de opção que corresponde aos critérios desejados da ACE na área Endereço IP de origem.

As opções são:

- Qualquer — Todos os endereços IPv6 de origem se aplicam à ACE.
- Definido pelo usuário — Insira um endereço IP e uma máscara curinga IP que devem ser aplicados à ACE nos campos *Source IP Address Value* e *Source IP Prefix Length*.

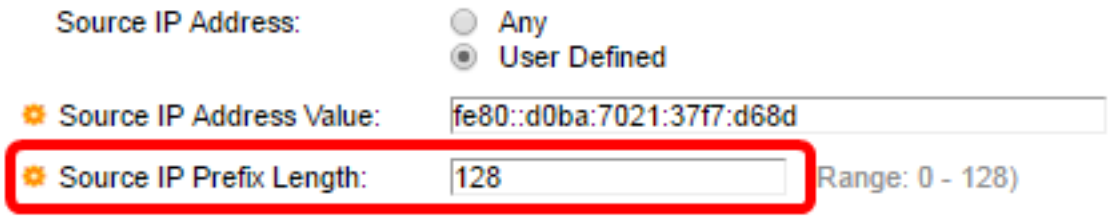
Note: Neste exemplo, Definido pelo usuário é escolhido. Se você escolheu Qualquer, vá para a Etapa 15.

Etapa 13. Insira o endereço IP origem no campo *Source IP Address Value*.



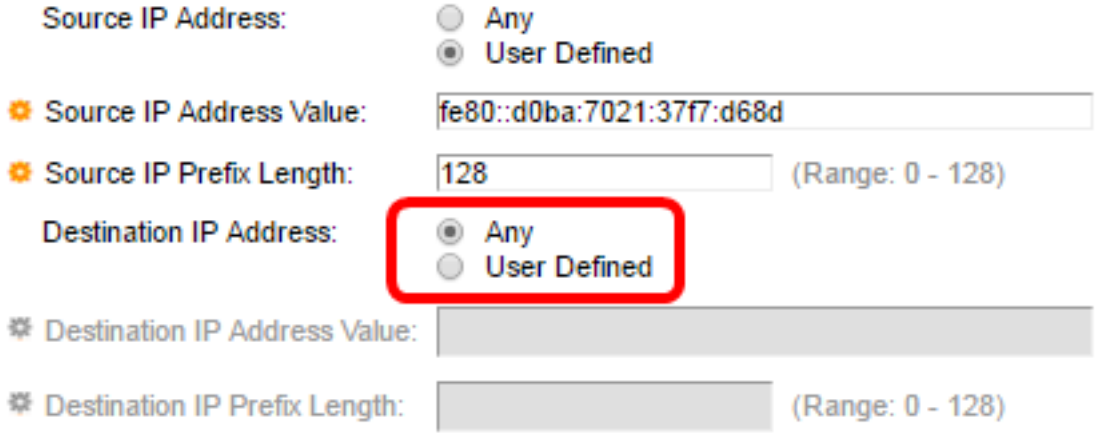
Note: Neste exemplo, fe80::d0ba:7021:37f7:d68d é usado.

Etapa 14. Insira o comprimento do prefixo IP de origem no campo *Tamanho do prefixo IP de origem*.



Note: Neste exemplo, 128 é usado.

Etapa 15. Clique no botão de opção que corresponde aos critérios desejados da ACE na área DestinationIP Address (Endereço IP de destino).

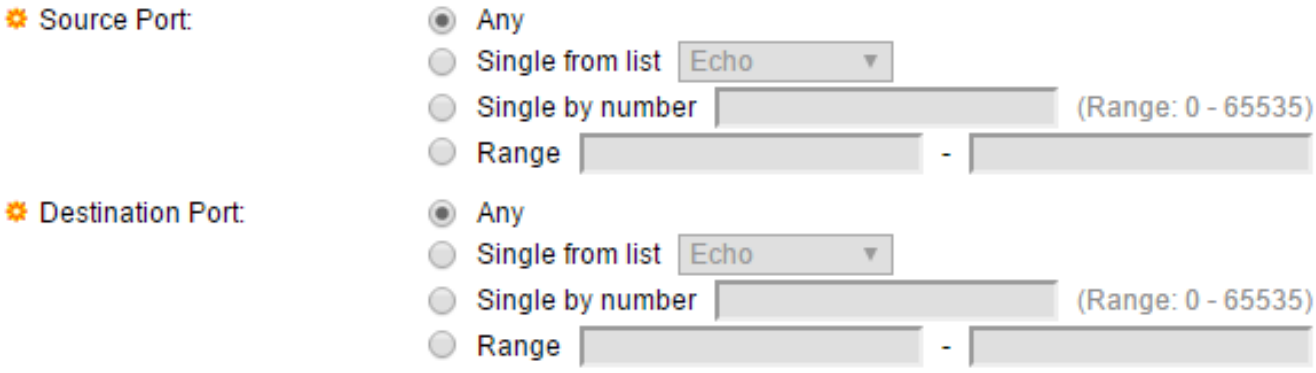


As opções são:

- Qualquer — Todos os endereços IPv6 de destino se aplicam à ACE.
- Definido pelo usuário — Insira um endereço IP e uma máscara curinga IP a serem aplicados à ACE nos campos *Destination IP Address Value* e *Destination IPPrefix Length*.

Note: Neste exemplo, Qualquer é escolhido. Escolher essa opção significa que a ACE a ser criada permitirá o tráfego da ACE que vem do endereço IPv6 especificado para qualquer destino.

Etapa 16. (Opcional) Clique em um botão de opção na área Porta de origem. O valor padrão é Qualquer.



- Qualquer - Corresponda a todas as portas de origem.
- Single from list — Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Um por número — Você pode escolher uma única porta de origem TCP/UDP à qual os

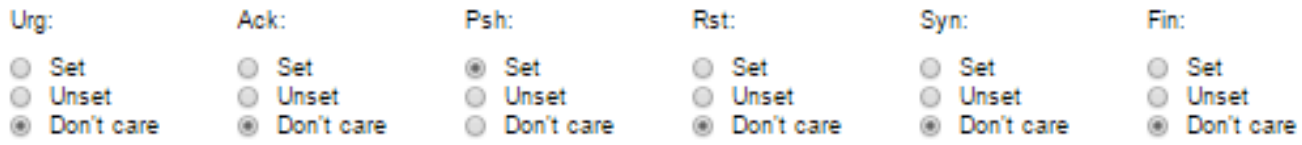
pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Intervalo — Você pode escolher um intervalo de portas origem TCP/UDP às quais o pacote corresponde. Há oito intervalos de porta diferentes que podem ser configurados (compartilhados entre as portas de origem e de destino). Cada um dos protocolos TCP e UDP tem oito intervalos de portas.

Etapa 17. (Opcional) Clique em um botão de opção na área Porta de destino. O valor padrão é Qualquer.

- Qualquer - Corresponda a todas as portas de origem
- Single from list — Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Um por número — Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Intervalo — Você pode escolher um intervalo de portas origem TCP/UDP às quais o pacote corresponde. Há oito intervalos de porta diferentes que podem ser configurados (compartilhados entre as portas de origem e de destino). Cada um dos protocolos TCP e UDP tem oito intervalos de portas.

Etapa 18. (Opcional) Na área Sinalizadores TCP, escolha um ou mais sinalizadores TCP com os quais filtrar pacotes. Os pacotes filtrados são encaminhados ou descartados. A filtragem de pacotes por flags TCP aumenta o controle de pacotes, o que aumenta a segurança da rede.

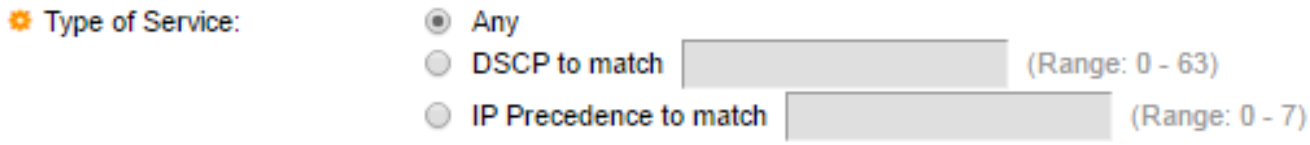
- Definir — Corresponder se o sinalizador estiver definido.
- Unset — Corresponde se o sinalizador não estiver definido.
- Não se importe — ignore o sinalizador TCP.



Os flags TCP são:

- Urg — Este sinalizador é usado para identificar os dados de entrada como Urgentes.
- Ack — Este sinalizador é usado para confirmar o recebimento bem-sucedido de pacotes.
- Psh — Esse sinalizador é usado para garantir que os dados recebam a prioridade (que merecem) e sejam processados na extremidade de envio ou recebimento.
- Rst — Esse flag é usado quando um segmento chega e não se destina à conexão atual.
- Syn — Este sinalizador é usado para comunicações TCP.
- Finalizar — Esse sinalizador é usado quando a comunicação ou a transferência de dados é concluída.

Etapa 19. (Opcional) Clique no tipo de serviço do pacote IP na área Tipo de serviço.



As opções são:

- Qualquer — Pode ser qualquer tipo de serviço para congestionamento de tráfego.
- DSCP para correspondência — O Differentiated Services Code Point é um mecanismo para classificar e gerenciar o tráfego de rede. Seis bits (0-63) são usados para selecionar o comportamento por salto de um pacote em cada nó.
- Precedência de IP para corresponder — a precedência de IP é um modelo de Tipo de Serviço (TOS) que a rede usa para ajudar a fornecer os compromissos de Qualidade de Serviço (QoS) apropriados. Esse modelo usa os três bits mais significativos do byte de tipo de serviço no cabeçalho IP, conforme descrito em RFC 791 e RFC 1349. A palavra-chave com valores de Preferência IP é a seguinte:

    - 0 — para rotina

    - 1 — para prioridade

    - 2 — para imediata

    - 3 — para flash

    - 4 — para flash-override

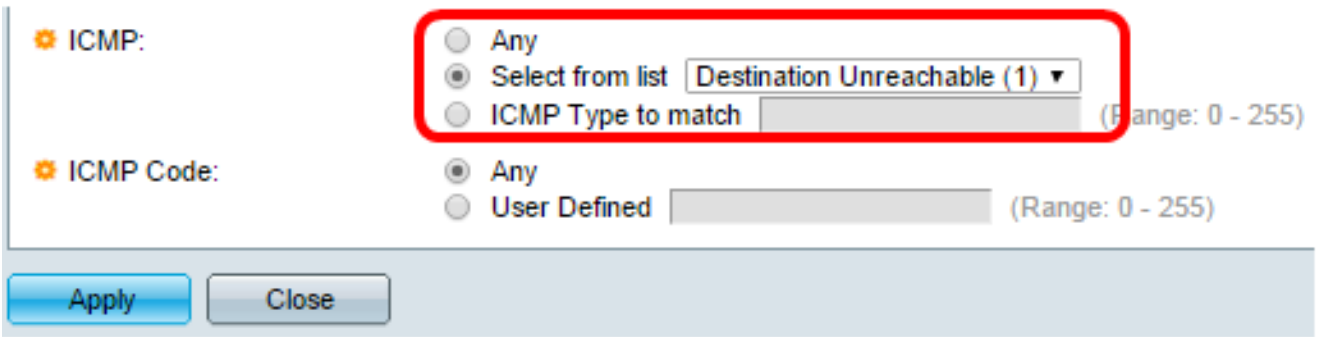
    - 5 — para críticos

    - 6 — para a internet

    - 7 — para a rede

Note: Neste exemplo, Qualquer é escolhido.

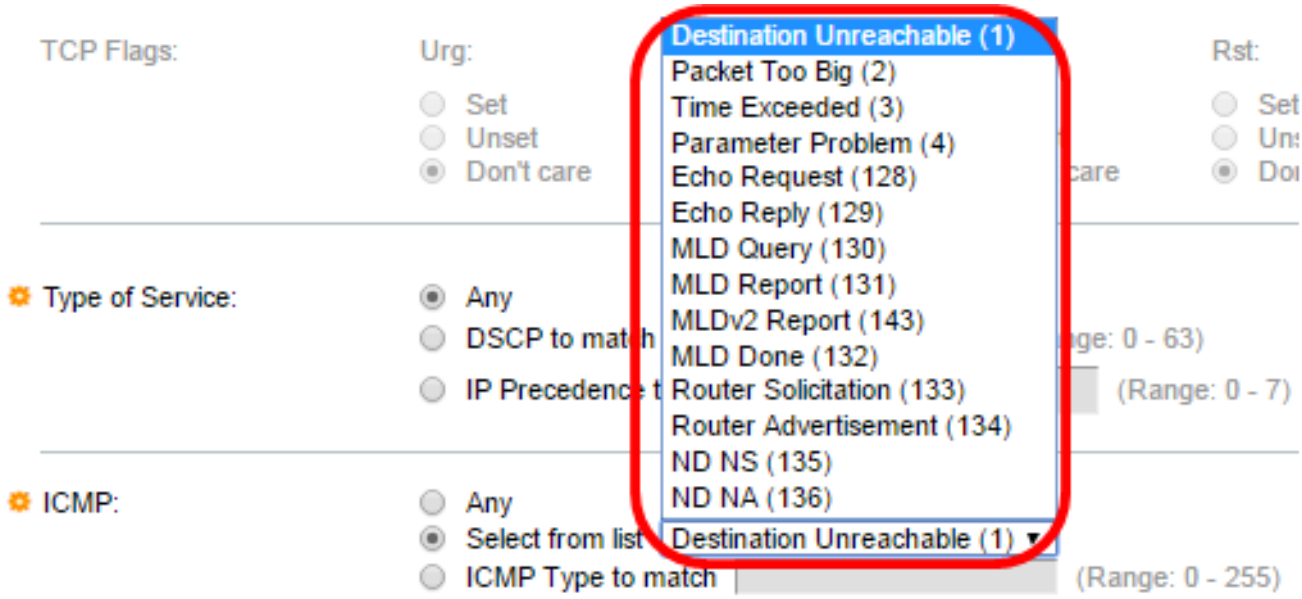
Etapa 20. (Opcional) Se o protocolo IP da ACL for ICMP, clique no tipo de mensagem ICMP usada para fins de filtragem. Escolha o tipo de mensagem por nome ou digite o número do tipo de mensagem:



- Qualquer — Todos os tipos de mensagem são aceitos.
- Selecionar na lista — Você pode escolher o tipo de mensagem por nome.
- Tipo de ICMP a corresponder — O número do tipo de mensagem a ser usado para fins de filtragem.

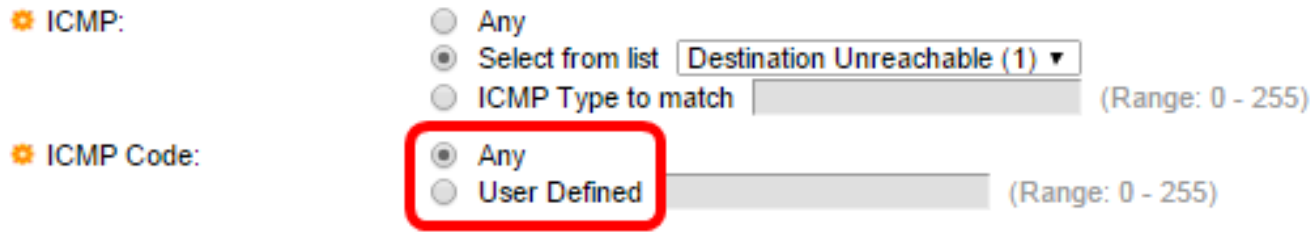
Note: Neste exemplo, a opção Selecionar na lista é escolhida.

Etapa 21. (Opcional) Se Select from list (Selecionar da lista) for escolhido na Etapa 20, escolha as mensagens de controle para filtrar nas opções possíveis na lista suspensa:



- Destino inalcançável (1) — É gerado pelo host ou seu gateway para informar ao cliente que o destino está inalcançável por algum motivo (exemplo: Erro inalcançável de rede ou host).
- Pacote muito grande (2) — O tamanho do datagrama excede o MTU especificado.
- Tempo excedido (3) — É gerado por um gateway para informar a origem de um datagrama descartado devido ao tempo de vida do campo que chega a zero.
- Parâmetro Problema (4) — Ele é gerado como resposta para qualquer erro não especificamente coberto por outra mensagem ICMP.
- Echo Request (128) — É um ping, cujos dados devem ser recebidos de volta em uma resposta de eco.
- Resposta de Eco (129) — É gerada em resposta a uma solicitação de eco.
- MLD Query (130) — É usado para saber quais endereços multicast têm ouvintes em um link conectado. Digite 130 em decimal.
- Relatório MLD (131) — É gerado quando o endereço multicast IPv6 ao qual o remetente da mensagem escuta.
- Relatório MLD v2 (143) — É igual ao relatório MLD com a versão 2.
- MLD concluído (132) — Quando o host sai de um grupo, ele envia uma mensagem de ouvinte de multicast para roteadores de multicast na rede.
- Solicitação de roteador (133) — É uma mensagem de descoberta de roteador. Os hosts descobrem os endereços de seus roteadores vizinhos simplesmente quando ouvem anúncios. O padrão é 224.0.0.2 para multicast; caso contrário, é 255.255.255.255.
- Anúncio de roteador (134) — O roteador envia periodicamente um anúncio de roteador de cada uma de suas interfaces multicast e anuncia os endereços IP dessa interface.
- ND NS (135) — As mensagens são originadas por nós para solicitar o endereço da camada de enlace de outro nó e também para funções como detecção de endereço duplicado e detecção de inacessibilidade de vizinhos.
- ND NA (136) — As mensagens são enviadas em resposta às mensagens NS. Se um nó alterar seu endereço da camada de link, ele poderá enviar um NA não solicitado para anunciar o novo endereço.

Etapa 22. (Opcional) As mensagens ICMP podem ter um campo de código que indica como tratar a mensagem. Isso é ativado se você escolher o protocolo ICMP na Etapa 10. Clique em uma das seguintes opções para configurar se deseja filtrar este código:

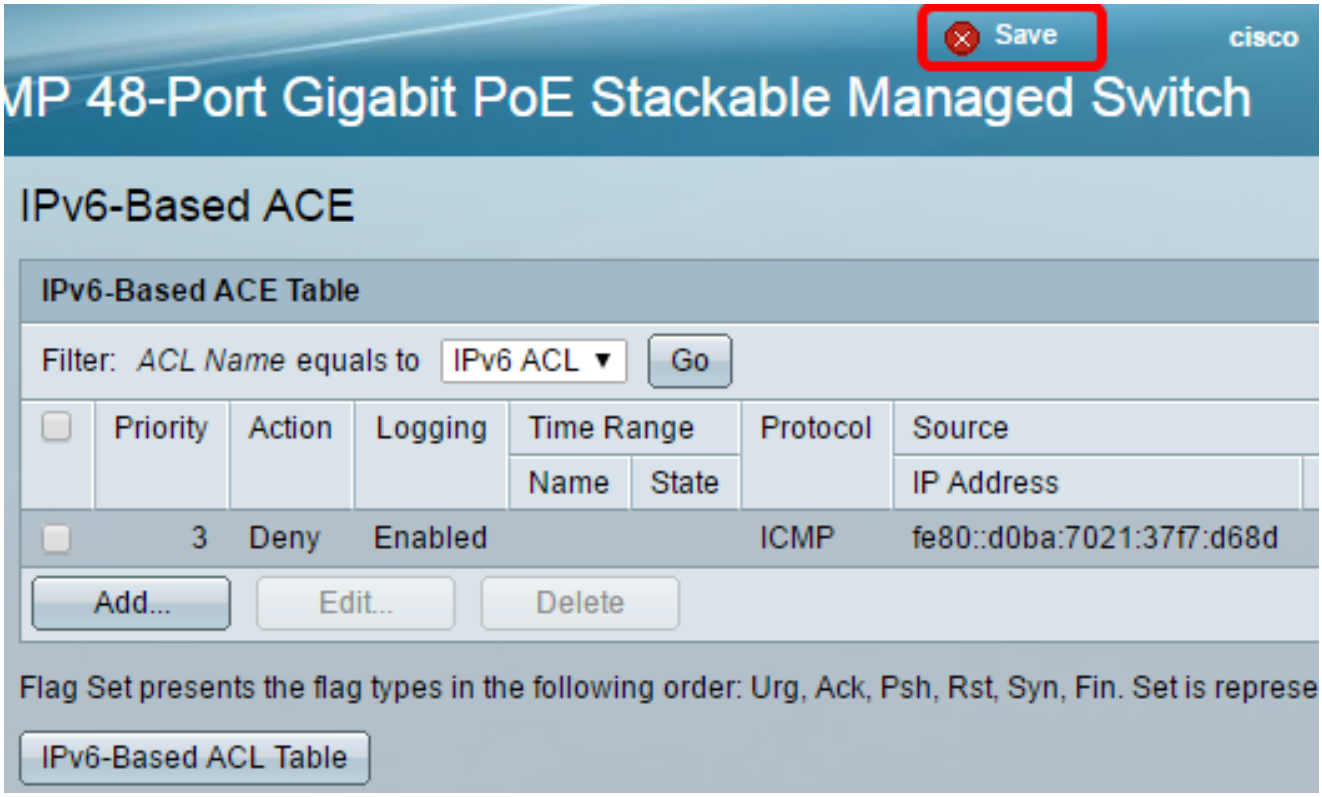


- Qualquer — Aceite todos os códigos.
- Definido pelo usuário — Você pode inserir um código ICMP para fins de filtragem.

Note: Neste exemplo, Qualquer é escolhido.

Etapa 23. Clique em **Aplicar** e, em seguida, clique em **Fechar**. A ACE é criada e associada ao nome da ACL.

Etapa 24. Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.



Agora você deve ter configurado uma ACE baseada em IPv6 no switch.