Criando uma ACL baseada em MAC no SG350XG e SG550XG

Objetivo

Uma lista de controle de acesso (ACL) é um conjunto de regras que podem ser criadas para manipular pacotes dependendo se eles atendem a determinados critérios. Esses critérios podem ser endereços origem ou destino, campos de cabeçalho e outros vários componentes de um pacote. Se um pacote corresponder aos critérios especificados de uma ACL, ele será descartado ou poderá continuar. Uma ACL baseada em MAC usa regras que analisam o cabeçalho da Camada 2 de um pacote para esses critérios, como endereços MAC, IDs de VLAN e valores de Ethertype. A implementação de uma ACL baseada em MAC permite controlar os pacotes que trafegam pelo switch no nível da Camada 2.

O objetivo deste documento é mostrar como criar e configurar uma ACL baseada em MAC nos switches SG350XG e SG550XG.

Dispositivos aplicáveis

- SG350XG
- SG550XG

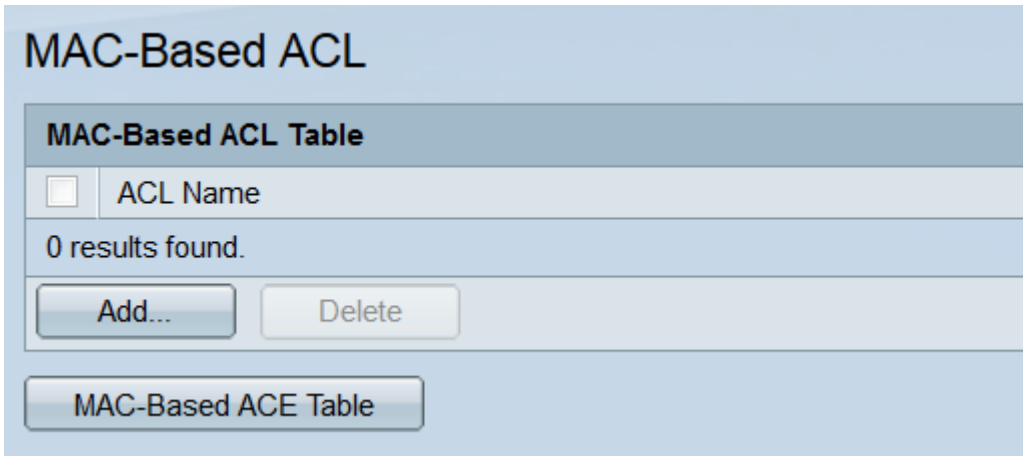
Versão de software

- v2.0.0.73

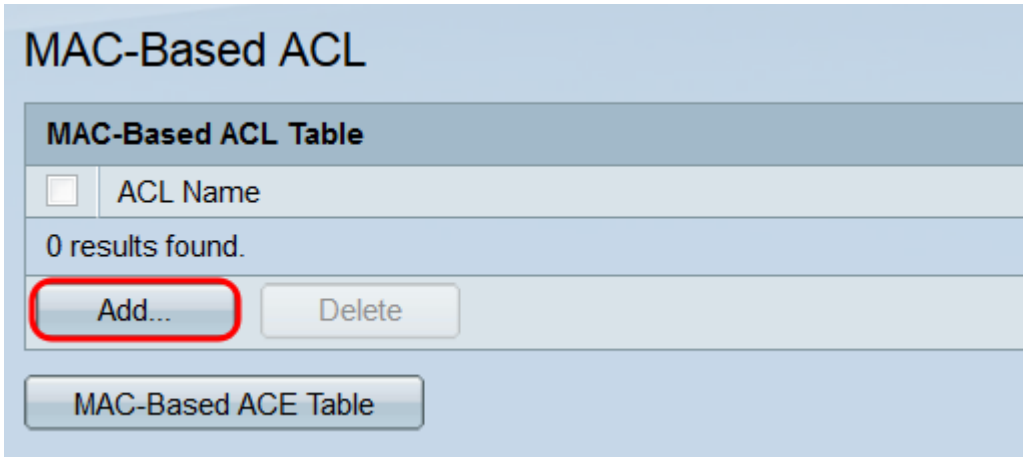
Configurando ACLs baseadas em MAC

Criando uma ACL e regras

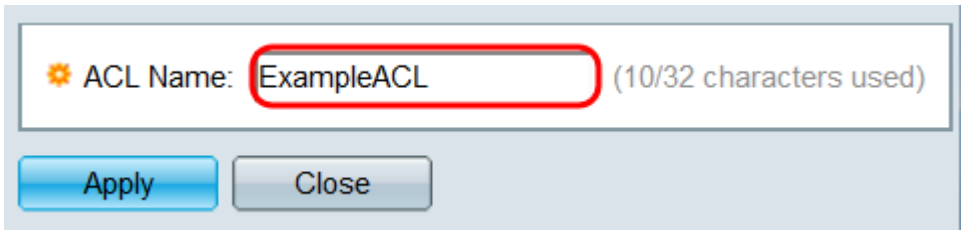
Etapa 1. Faça login no utilitário de configuração da Web e escolha **Controle de acesso > ACL baseada em MAC**. A página *ACL baseada em MAC* é aberta.



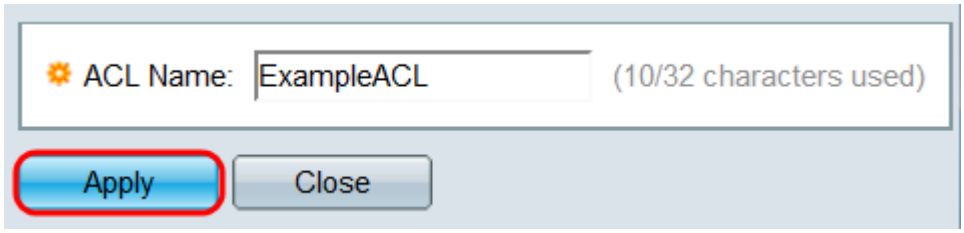
Etapa 2. A *Tabela de ACLs baseadas em MAC* exibirá todas as ACLs baseadas em MAC atualmente no switch. Para criar uma nova ACL, clique no botão **Adicionar...**. A janela *Add MAC-Based ACL* será aberta.



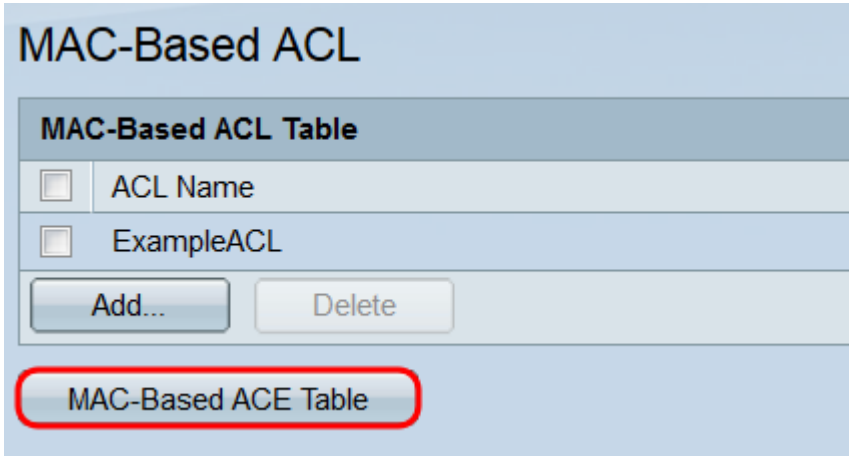
Etapa 3. No campo *ACL Name*, digite o nome da nova ACL. Esse nome não afetará a função da ACL e é somente para fins de identificação.



Etapa 4. Clique em Apply. A nova ACL será adicionada à *tabela de ACL baseada em MAC*. Clique em **Fechar** para retornar à página *ACL baseada em MAC* ou criar outra ACL repetindo a etapa anterior.

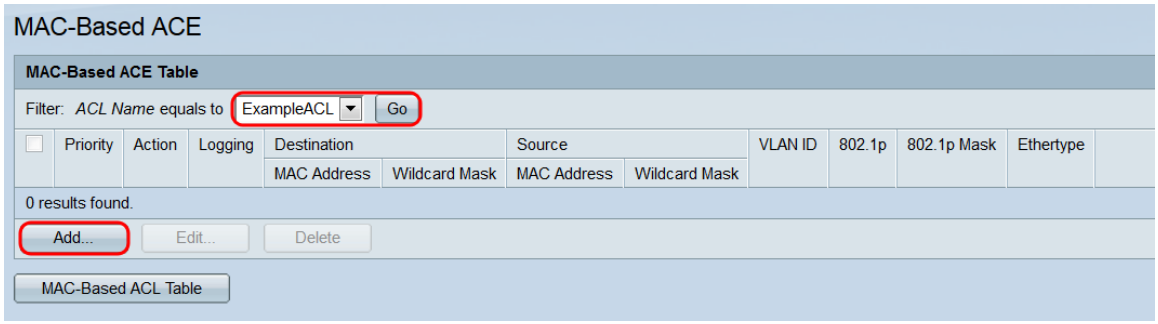


Etapa 5. Qualquer ACL recém-criada estará vazia; ou seja, não conterá nenhuma regra para bloquear ou permitir pacotes com base em endereços MAC. Para criar essas regras, uma entrada de controle de acesso (ACE) deve ser adicionada à ACL. Para fazer isso, clique no botão **Tabela de ACE Baseada em MAC** para ir para a página *ACE Baseada em MAC*.

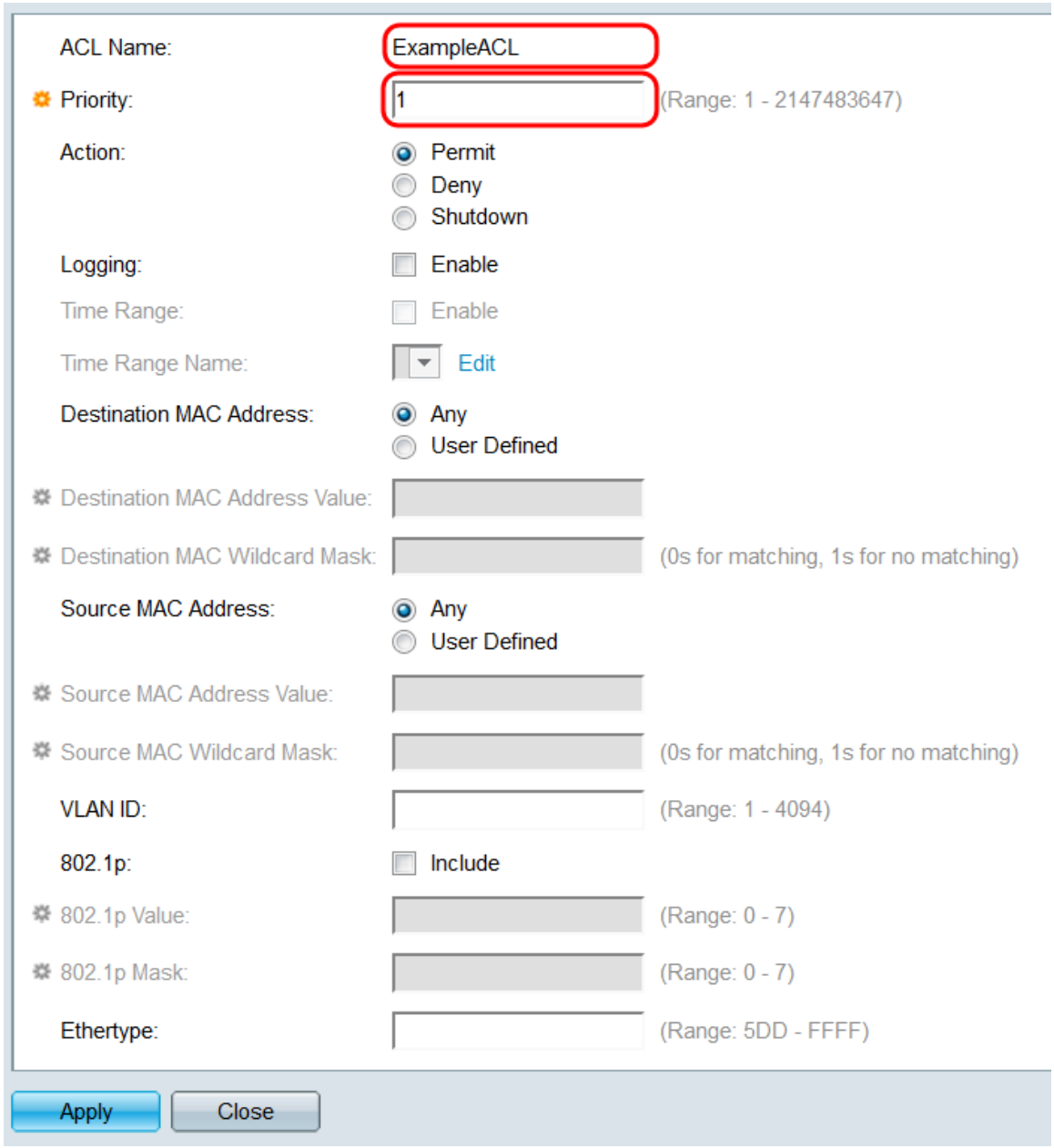


Etapa 6. Na página *ACE baseada em MAC*, selecione a ACL à qual deseja adicionar uma ACE por meio da lista suspensa na parte superior da *Tabela ACE baseada em MAC* e clique em **Ir**. A tabela exibe todas as ACEs atualmente associadas à ACL selecionada. Para

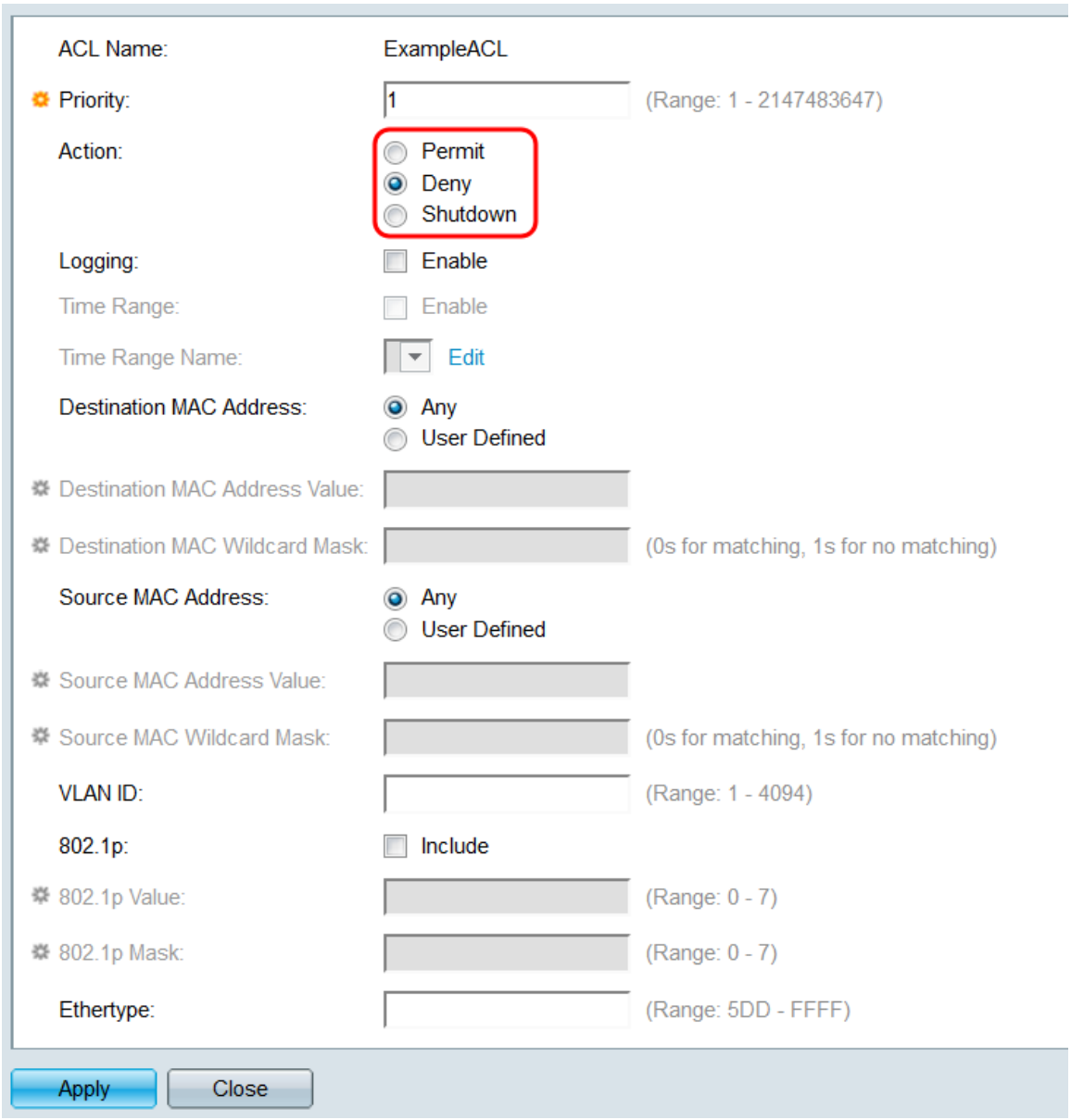
adicionar uma ACE, clique no botão **Adicionar...**. A janela *Add MAC-Based ACE* será aberta.



Passo 7. O campo *ACL Name* exibirá o nome da ACL à qual você está adicionando uma ACE. No campo *Prioridade*, insira um número de prioridade para a ACE. Quanto maior a prioridade de uma ECA, mais rápido ela será processada. O intervalo é de 1 a 2147483647, sendo 1 a prioridade mais alta.



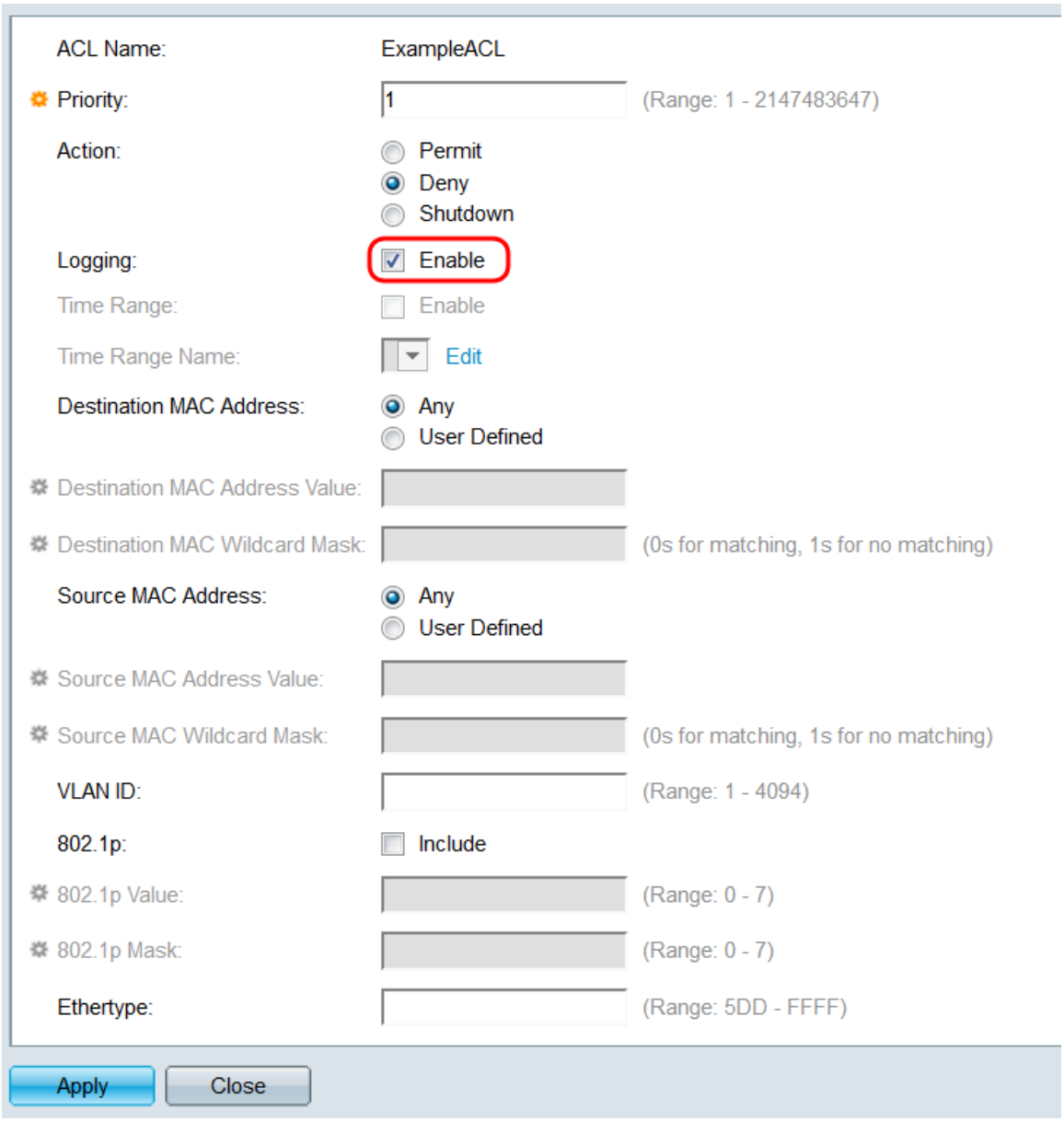
Etapa 8. No campo *Ação*, selecione um botão de opção para determinar o que acontecerá quando os critérios da ECA forem atendidos.



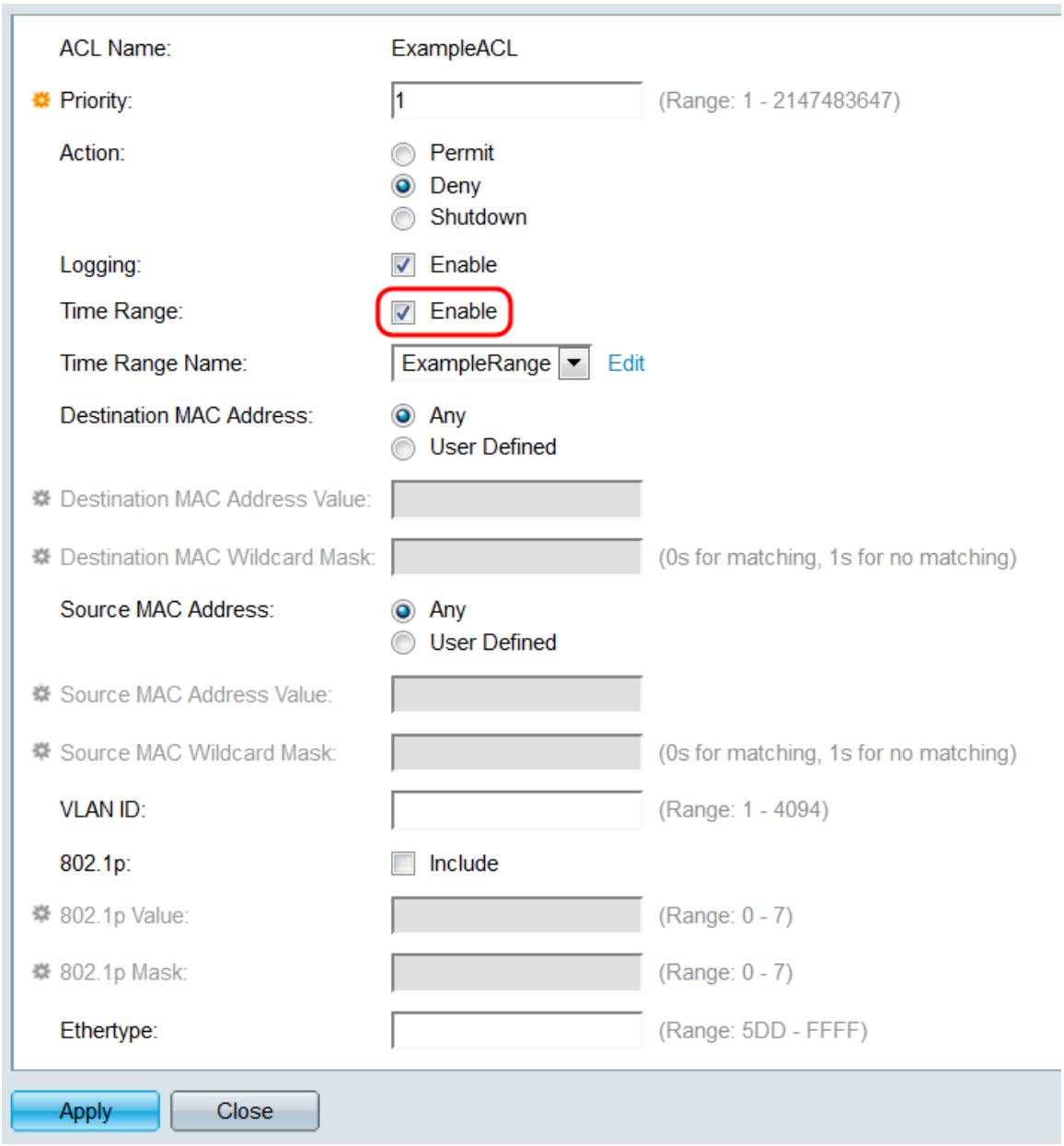
As opções são:

- Permit (Permitir) - Forward packets que atendem aos critérios.
- Negar - Descarte os pacotes que atendem aos critérios.
- Desligamento - Descarte os pacotes que atendem aos critérios e desative a porta.

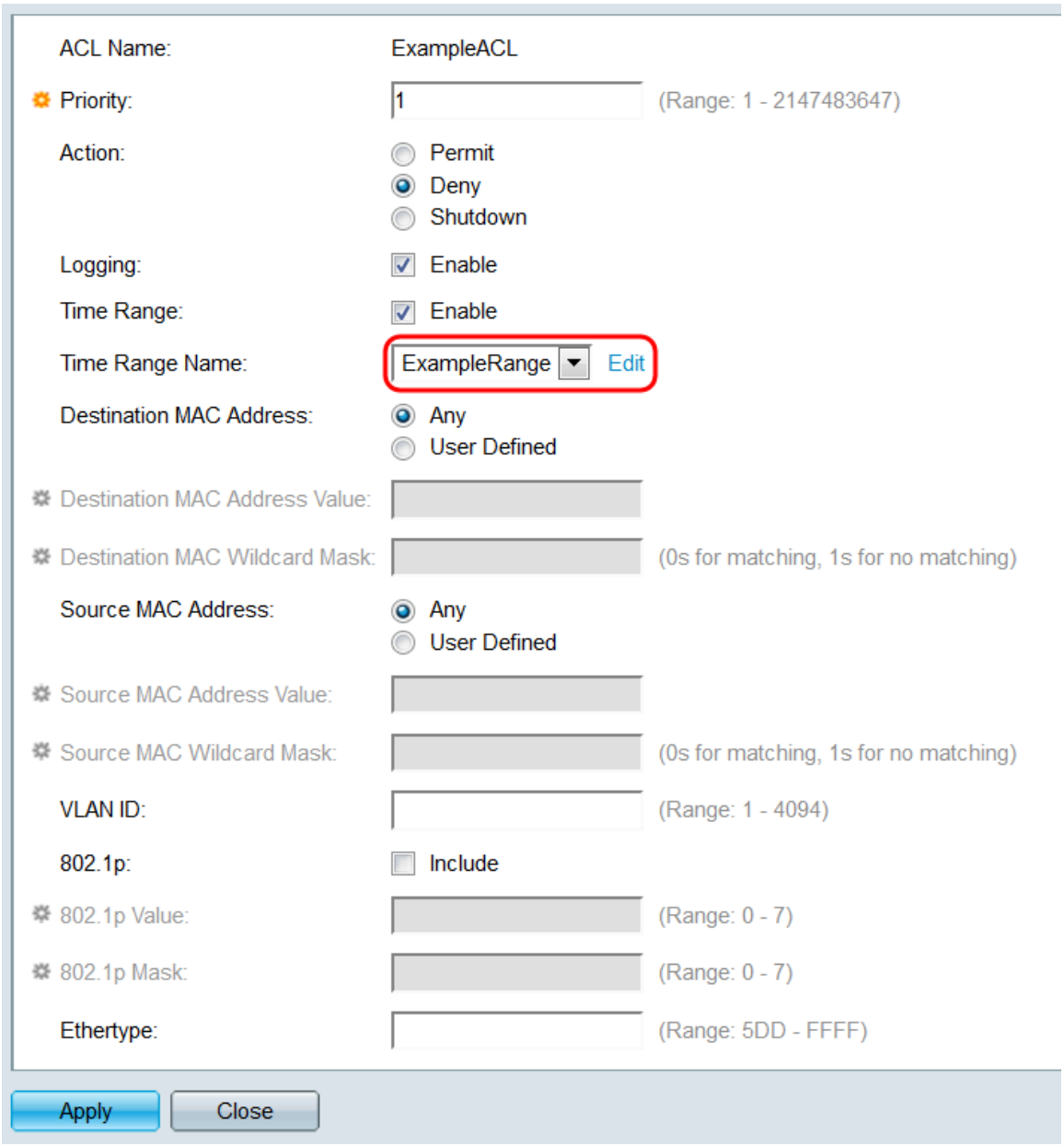
Etapa 9. No campo *Logging*, marque a caixa de seleção **Enable** para ativar os fluxos de ACL de registro correspondentes à regra ACE. Se estiver usando o modo de exibição Básico, vá para a Etapa 12. O modo de exibição pode ser alterado através da lista suspensa no canto superior direito do utilitário da Web.



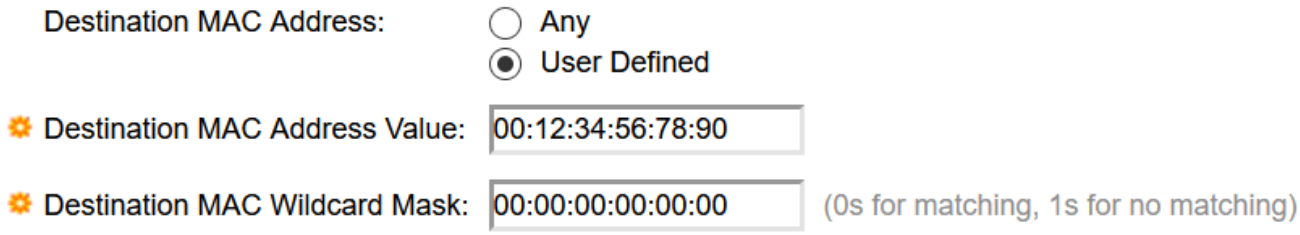
Etapa 10. No campo *Intervalo de tempo*, marque a caixa de seleção **Habilitar** para que a ACE só esteja ativa durante um intervalo de tempo especificado. Se não houver intervalos de tempo configurados no switch, esse campo ficará indisponível.



Etapa 11. Se você ativou um intervalo de tempo para esta ACE, o campo *Nome do intervalo de tempo* estará disponível. Use a lista suspensa para selecionar um intervalo de tempo já configurado no switch para aplicar à ACE. Se não houver intervalos de tempo no switch, esse campo ficará indisponível; clique no link **Editar** para ir para a página *Intervalo de tempo* para criar ou modificar intervalos de tempo. Para obter mais informações, consulte o artigo *Setting Up a Time Range (Configuração de um intervalo de tempo) no SG350XG e no SG550XG*.



Etapa 12. No campo *Endereço MAC de Destino*, selecione um botão de opção para determinar que endereços MAC de destino constituirão uma correspondência. Selecione **Qualquer** para que qualquer endereço de destino seja uma correspondência ou **Definido pelo usuário** para especificar um endereço ou intervalo de endereços.



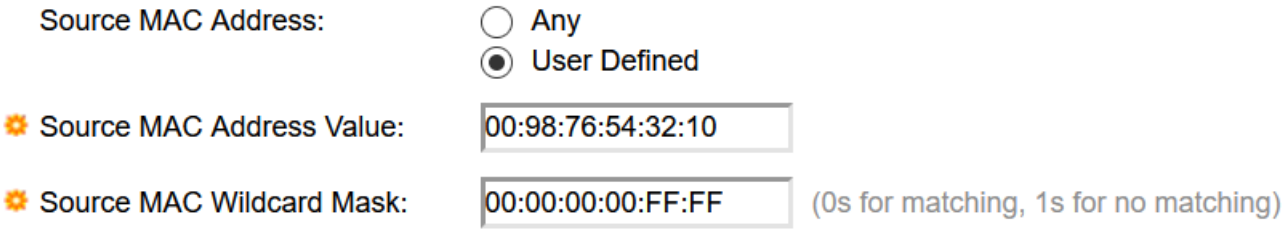
Se você selecionou **Definido pelo usuário**, preencha os seguintes campos:

- Valor do endereço MAC de destino - Insira o endereço MAC de destino. Se um pacote contiver esse endereço de destino, a ACE o considerará uma correspondência.
- Máscara Curinga MAC de Destino - Insira uma máscara para definir um intervalo de endereços. Definir um bit como 1 fará com que o bit correspondente no endereço MAC seja

ignorado, e 0 será correspondente a bits.

Nota: Dada uma máscara de 0000 0000 0000 0000 0000 0000 0000 0000 000 0000 111 1111 (o que significa que você corresponde nos bits onde s 0 e não correspondem nos bits onde há 1's). Você precisa converter os 1 em um valor hexadecimal e escrever 0 para cada quatro zeros. Neste exemplo, desde 1111 1111 = FF, a máscara seria escrita: como 00:00:00:00:00:FF.

Etapa 13. No campo *Endereço MAC de Origem*, selecione um botão de opção para determinar que endereços MAC de origem constituirão uma correspondência. Selecione **Qualquer** para que qualquer endereço de origem seja uma correspondência ou **Definido pelo usuário** para especificar um endereço ou intervalo de endereços.



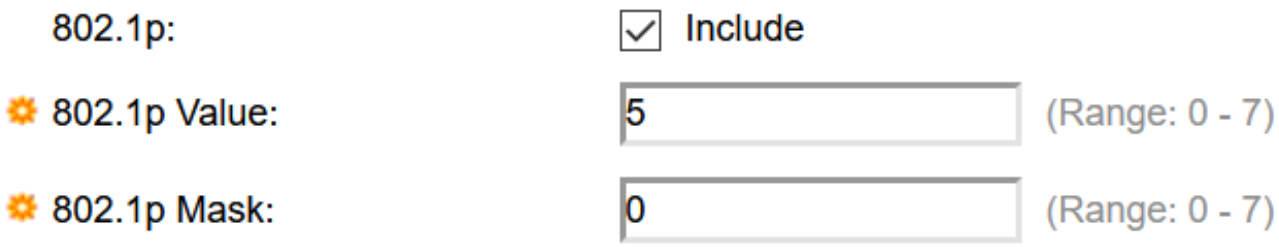
Se você selecionou **Definido pelo usuário**, preencha os seguintes campos:

- Valor do endereço MAC de origem - Insira o endereço MAC de origem. Se um pacote contiver esse endereço de origem, a ACE considerará uma correspondência.
- Máscara Curinga MAC de Origem - Insira uma máscara para definir um intervalo de endereços. Definir um bit como 1 fará com que o bit correspondente no endereço MAC seja ignorado, e 0's corresponderá aos bits (por exemplo, 00:00:00:00:00:11).

Nota: Dada uma máscara de 0000 0000 0000 0000 0000 0000 0000 0000 000 0000 111 1111 (o que significa que você corresponde nos bits onde s 0 e não correspondem nos bits onde há 1's). Você precisa converter os 1 em um valor hexadecimal e escrever 0 para cada quatro zeros. Neste exemplo, desde 1111 1111 = FF, a máscara seria escrita: como 00:00:00:00:00:FF.

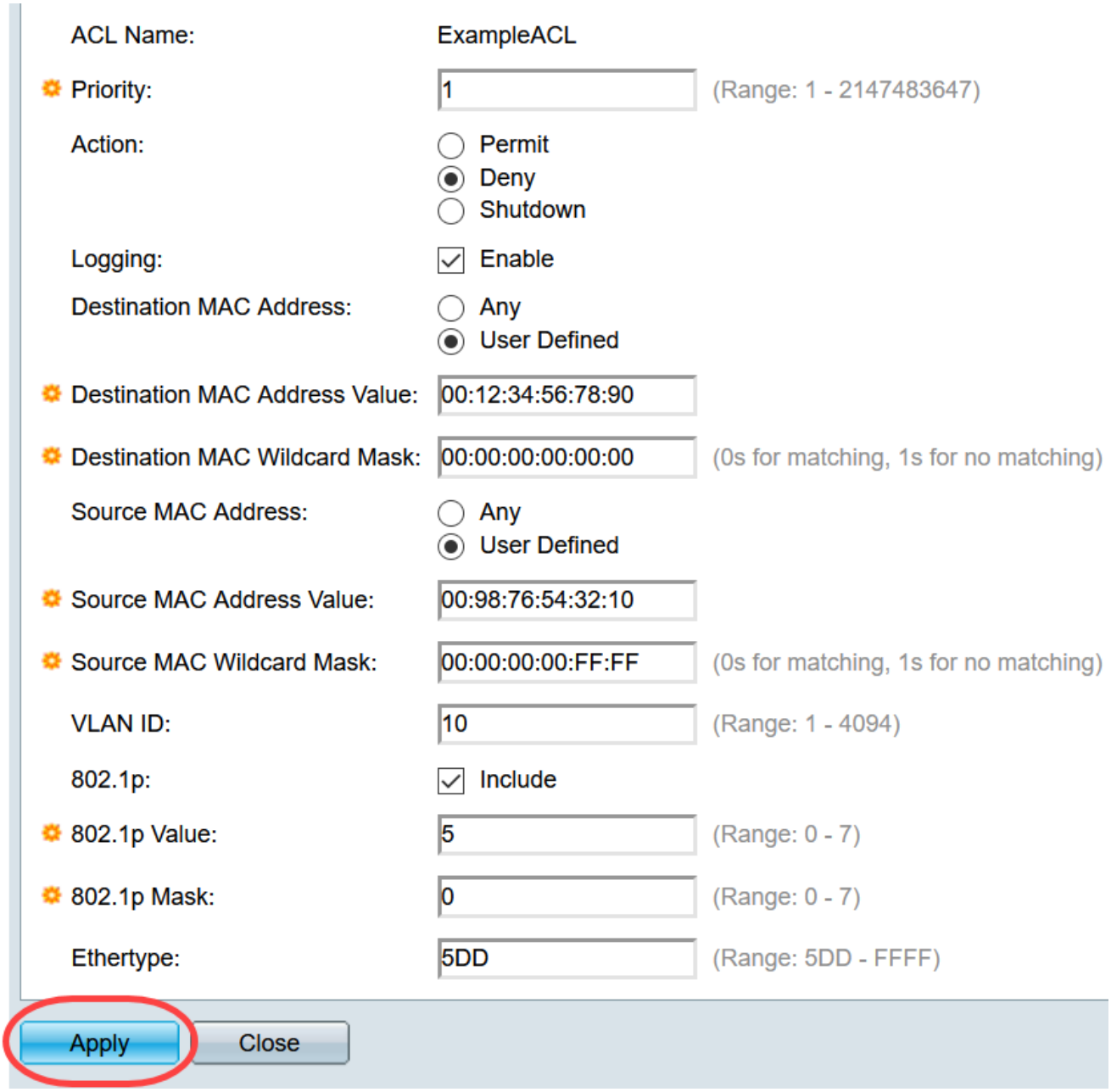
Etapa 14. No campo *VLAN ID*, insira um VLAN ID de 1 a 4094. Se um pacote contiver essa ID de VLAN, a ACE considerará uma correspondência. Este campo não é obrigatório; deixar em branco fará com que a ACE não considere as IDs de VLAN ao examinar pacotes.

Etapa 15. No campo *802.1p*, marque a caixa de seleção **Incluir** para que a ACE inclua critérios 802.1p. Se você incluiu critérios 802.1p, insira um valor 802.1p e uma máscara nos campos *Valor 802.1p* e *Máscara 802.1p*, respectivamente. O intervalo para ambos os campos é de 0 a 7. Se um pacote contiver o valor 802.1p correspondente e se ajustar à máscara, a ACE considerará uma correspondência.



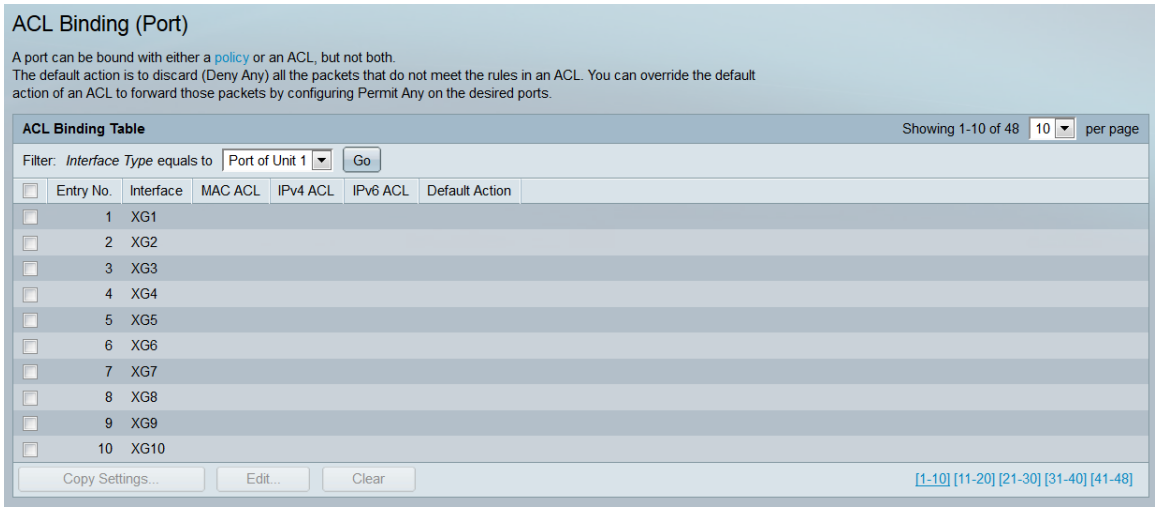
Etapa 16. No campo *Ethertype*, insira um valor Ethertype que será comparado aos pacotes de entrada. Ethertype é um campo de dois octetos em um quadro que indica qual protocolo é encapsulado no pacote. O intervalo é 5DD- FFFF. Se um pacote contiver o valor Ethertype especificado, a ACE considerará uma correspondência. Uma lista de valores Ethertype pode ser encontrada nesta página de padrões IEEE.

Etapa 17. Clique em Apply. A ACE será adicionada à ACL especificada. Clique em **Fechar** para retornar à página *ACE baseada em MAC*.

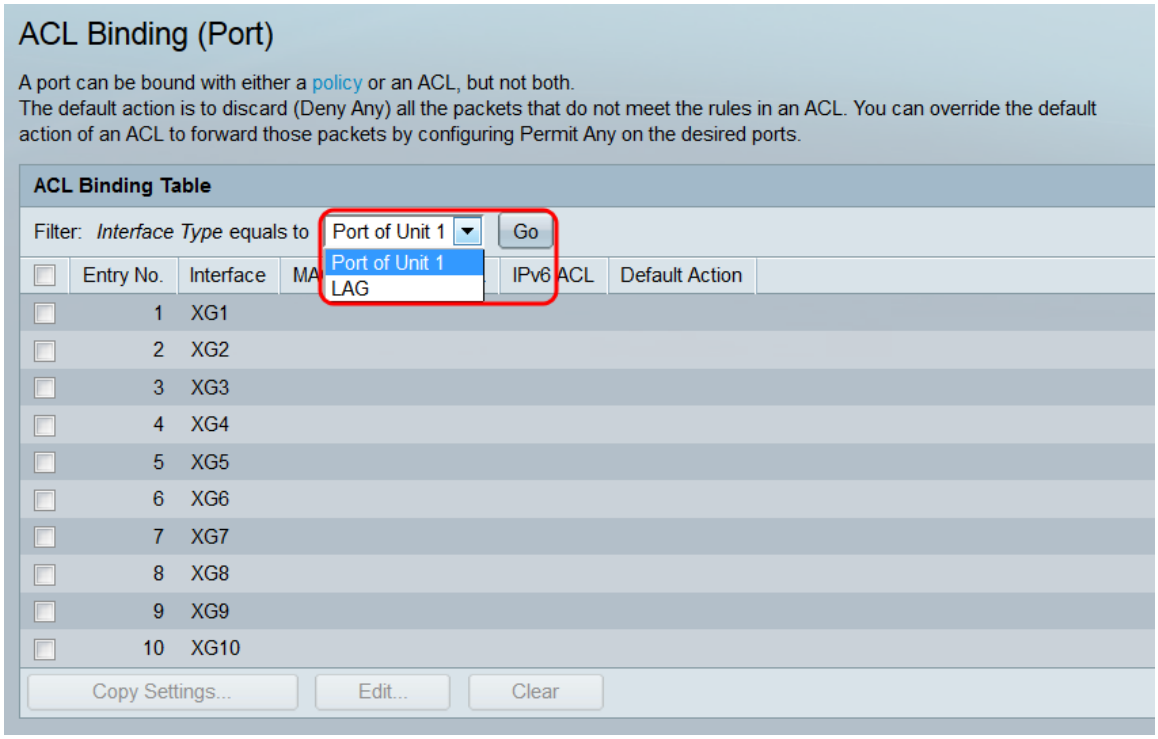


Mapeamento de uma ACL baseada em MAC às portas

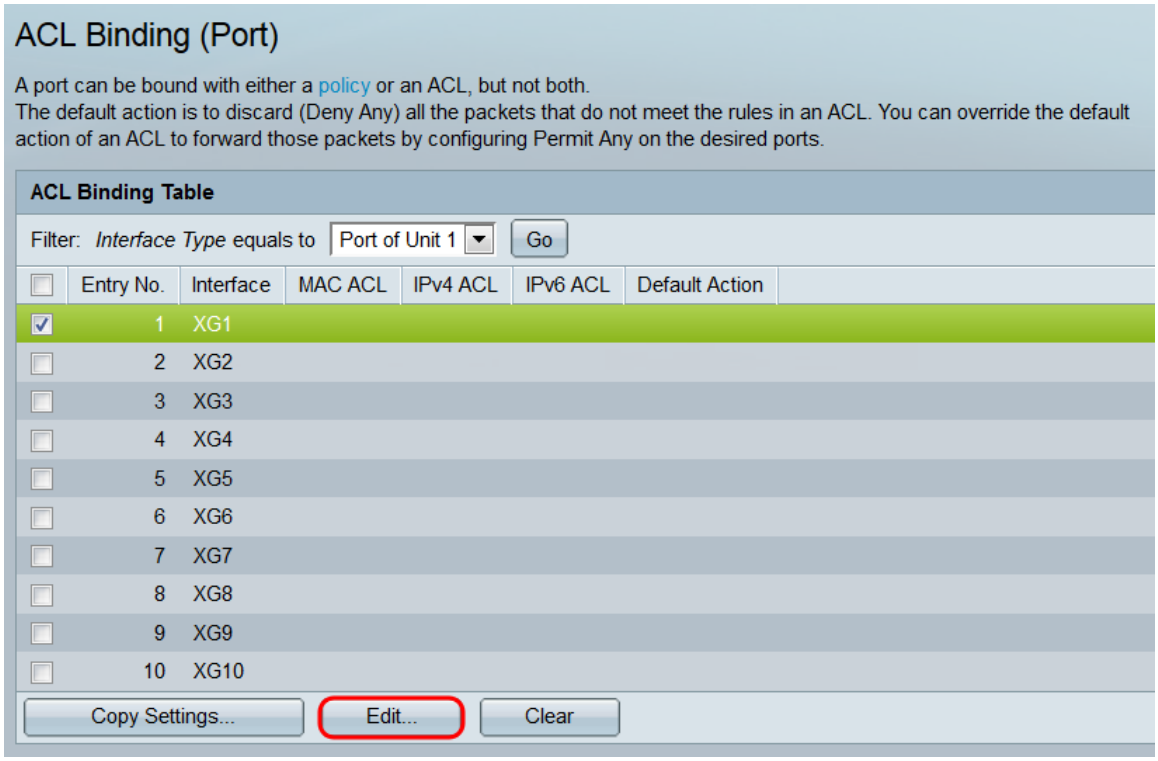
Etapa 1. Uma ACL pode ser mapeada para portas ou VLANs. Para mapear uma ACL baseada em MAC para uma porta ou portas, navegue para **Controle de acesso > Vinculação de ACL (Porta)**. A página *ACL Binding (Port)* é aberta.



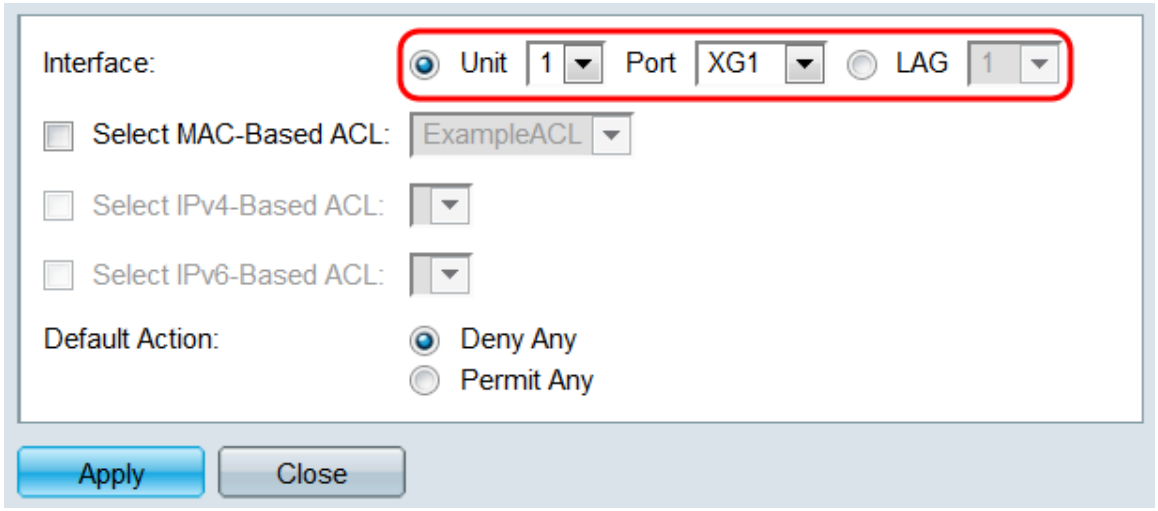
Etapa 2. Na lista suspensa na parte superior da *Tabela de vinculação de ACL*, selecione portas ou LAG (grupo de agregação de links) como um tipo de interface. Se o switch fizer parte de uma pilha, as portas de outras unidades poderão ser selecionadas. Clique em **Ir** para exibir uma lista do tipo de interface especificado.



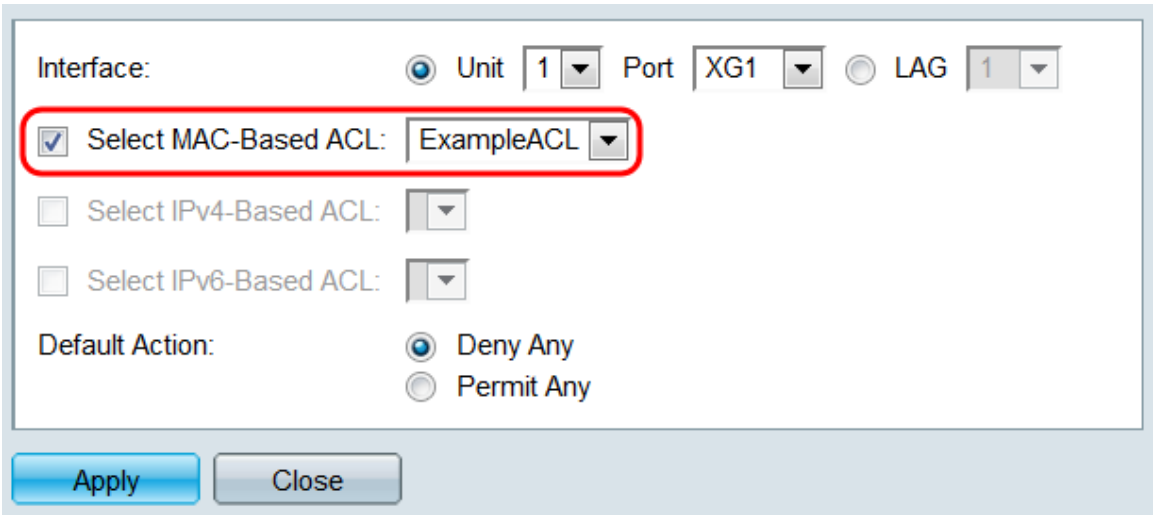
Etapa 3. Marque a caixa de seleção de uma interface e clique no botão **Editar...**. A janela *Edit ACL Binding* é aberta.



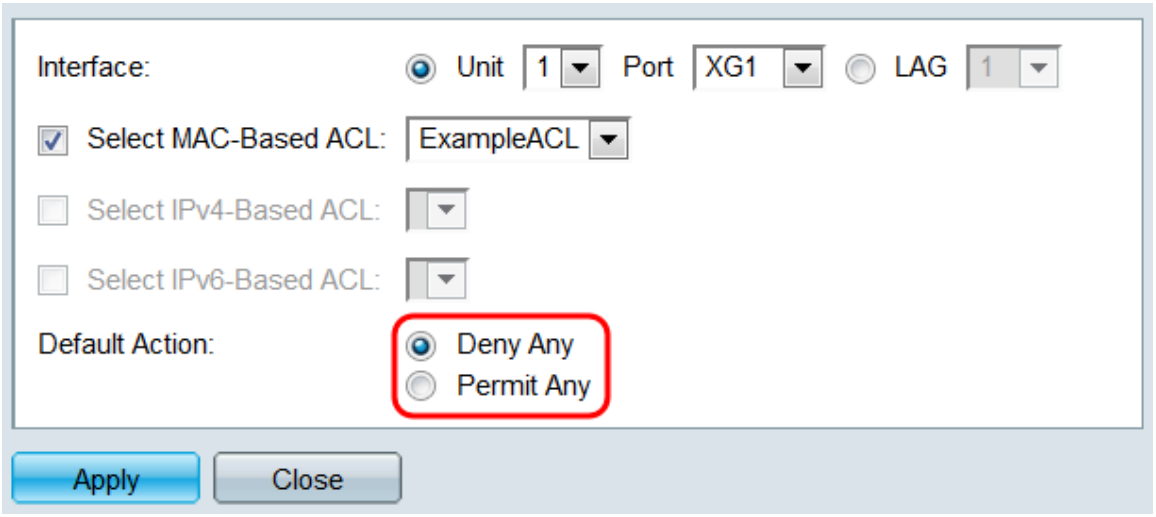
Etapa 4. O campo *Interface* exibe a porta ou o LAG que está sendo configurado no momento. Ele exibirá automaticamente a interface selecionada na *Tabela de Associação de ACL*. Esse campo pode ser usado para alternar rapidamente entre diferentes interfaces sem voltar à página *ACL Binding (Port)*.



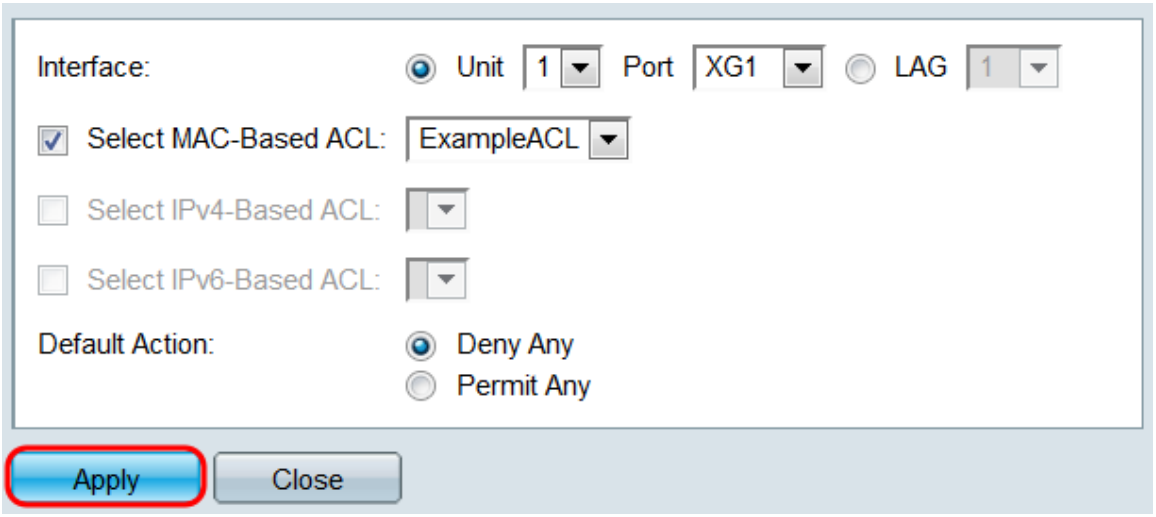
Etapa 5. Marque a caixa de seleção **Select MAC-Based ACL** e use a lista suspensa para selecionar uma ACL para mapear para a interface especificada.



Etapa 6. No campo *Ação padrão*, selecione um botão de opção para determinar como os pacotes que não correspondem aos critérios da ACL serão tratados. O padrão é **Deny Any**, que descarta todos os pacotes que não correspondem aos critérios da ACL; **Permitir qualquer** encaminhará pacotes não correspondentes.

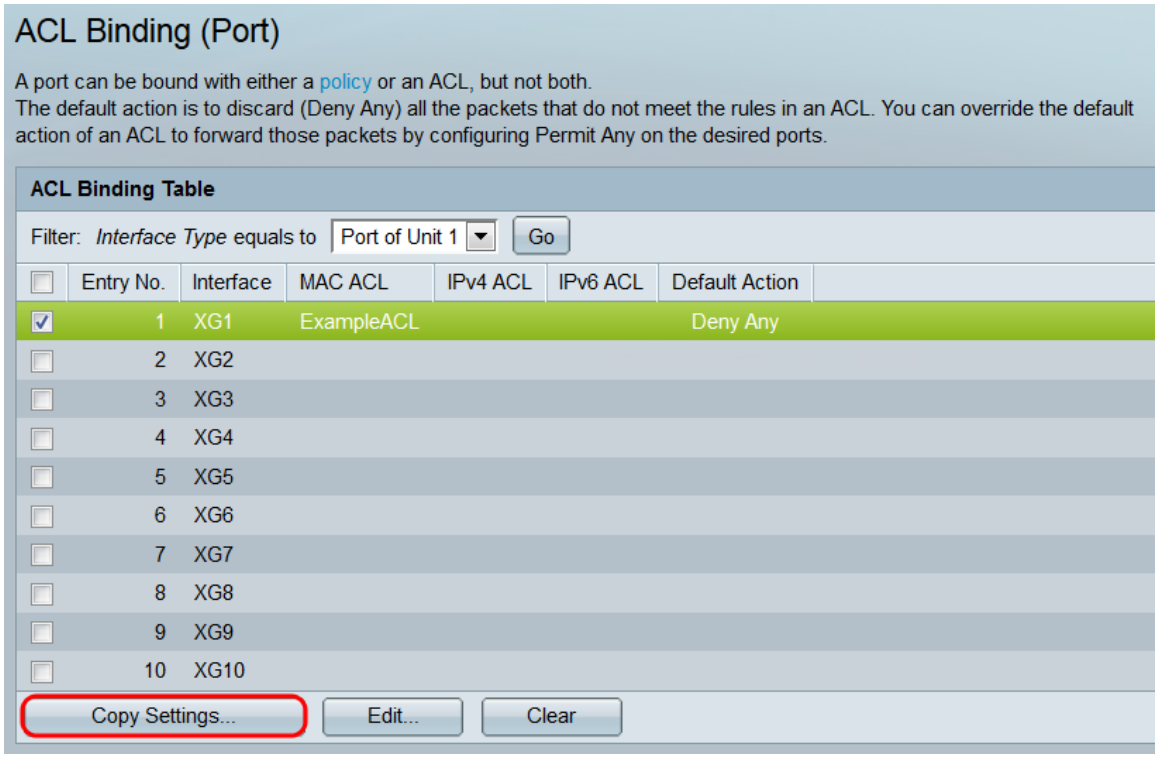


Passo 7. Clique em Apply. A ACL é mapeada para a interface especificada. Você pode usar o campo *Interface* para selecionar uma interface diferente para configurar ou clicar em **Fechar** para retornar à página *ACL Binding (Port)*.

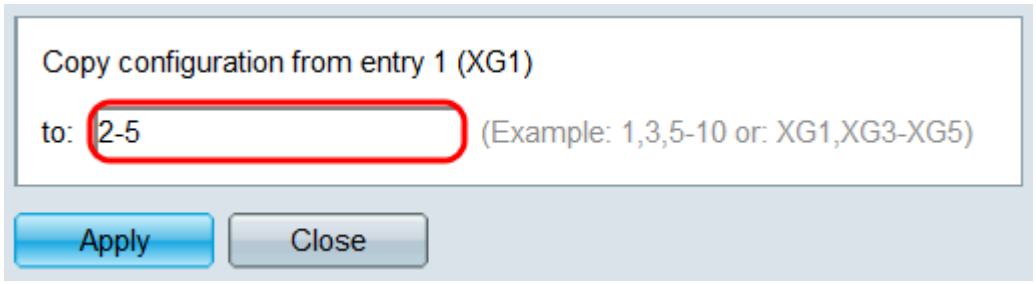


Etapa 8. Para copiar rapidamente as configurações de uma interface para outras interfaces, marque a caixa de seleção da interface que deseja copiar e clique no botão **Copiar**

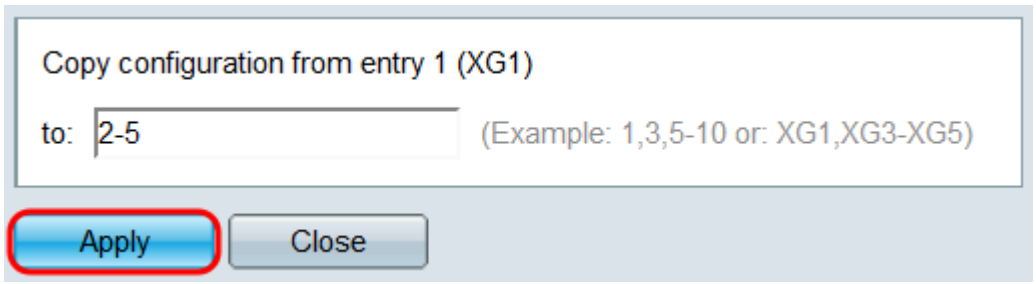
configurações.... A janela *Copiar configurações* é aberta.



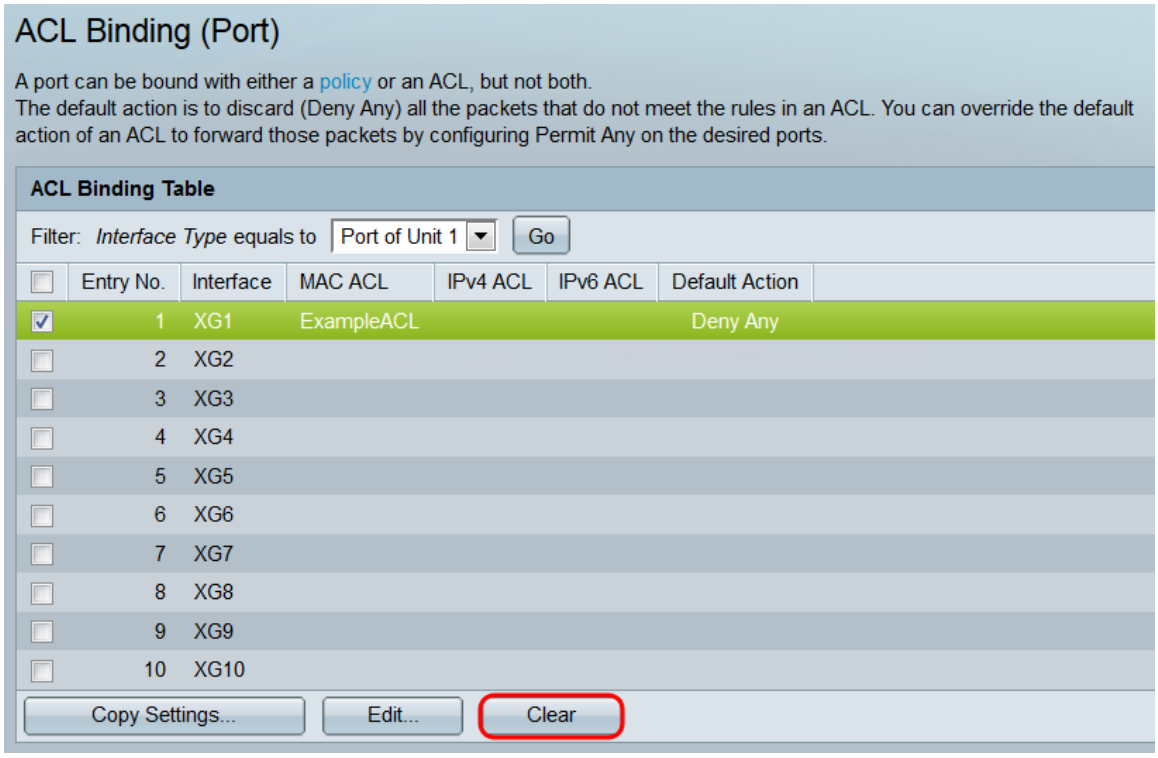
Etapa 9. No campo de texto, insira a interface ou as interfaces para as quais deseja copiar as configurações. As interfaces podem ser separadas por vírgulas ou um intervalo pode ser especificado.



Etapa 10. Clique em Apply. As configurações são copiadas.

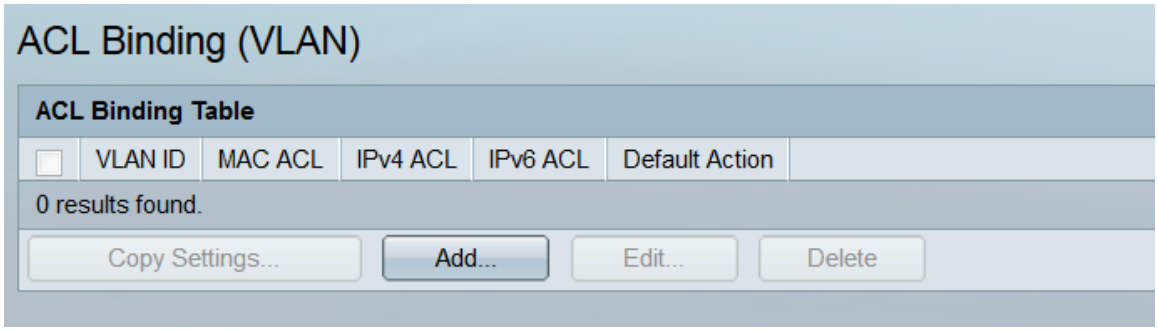


Etapa 11. Se desejar limpar as configurações de uma interface, marque a caixa de seleção e clique em **Limpar**. Observe que várias interfaces podem ser selecionadas e limpas simultaneamente.

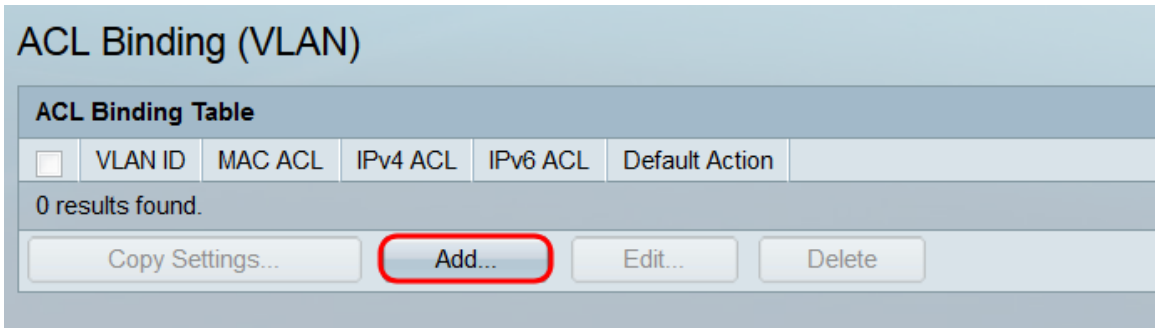


Mapeamento de uma ACL baseada em MAC para VLANs

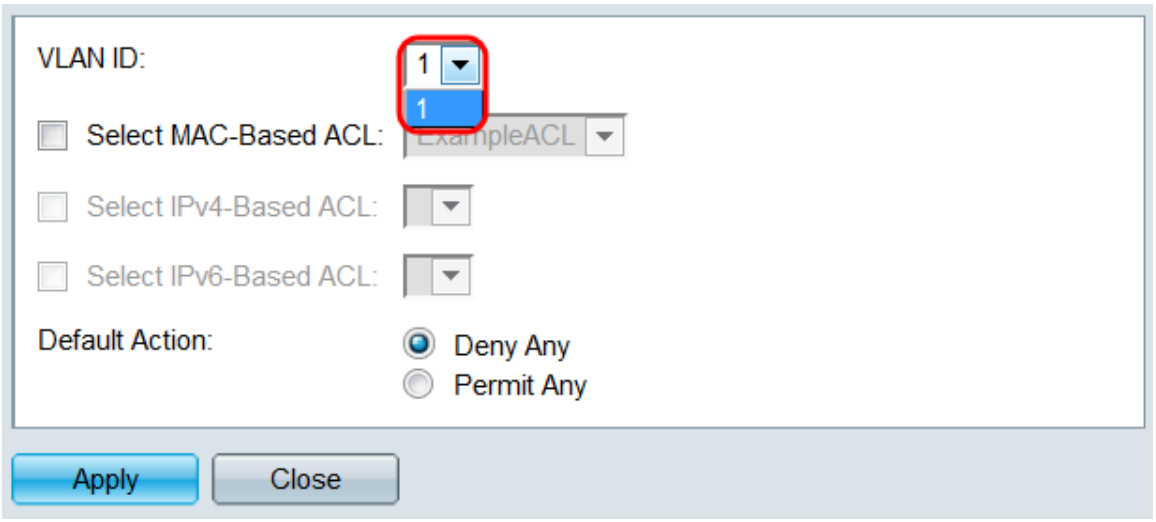
Etapa 1. Uma ACL pode ser mapeada para portas ou VLANs. Para mapear uma ACL baseada em MAC para uma VLAN, navegue para **Controle de acesso > Vinculação de ACL (VLAN)**. A página *ACL Binding (VLAN)* é aberta.



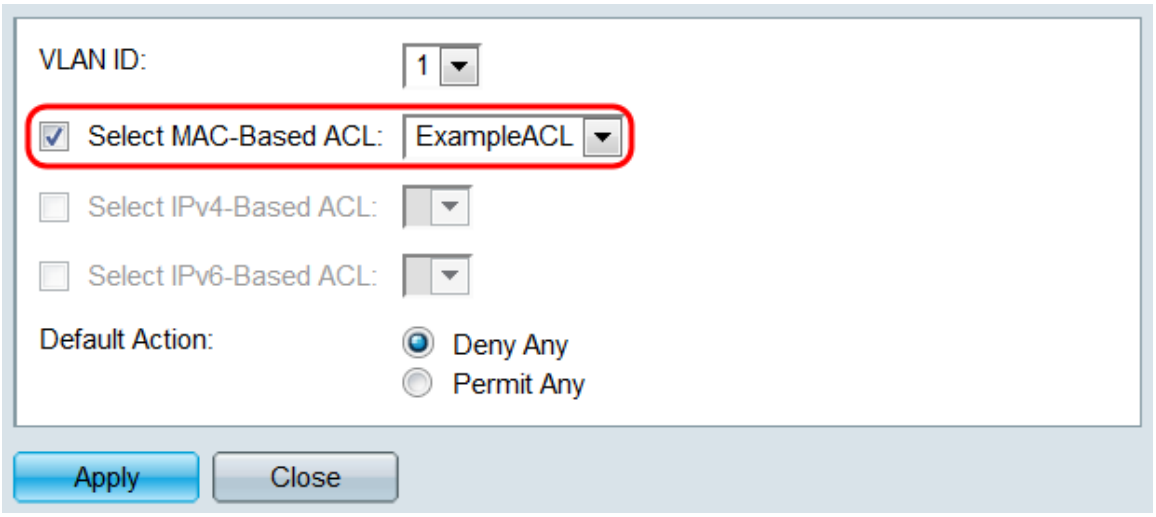
Etapa 2. A *Tabela de Associação de ACL* exibe todas as ACLs mapeadas atualmente para VLANs. Se nenhuma ACL foi mapeada, a tabela está vazia. Para mapear uma ACL para uma VLAN, clique no botão **Adicionar...**. A janela *Add ACL Binding* é aberta.



Etapa 3. Selecione uma VLAN para mapear uma ACL para usar a lista suspensa no campo *VLAN ID*. Esse campo também pode ser usado para alternar rapidamente entre diferentes VLANs sem voltar à página *ACL Binding (VLAN)*.

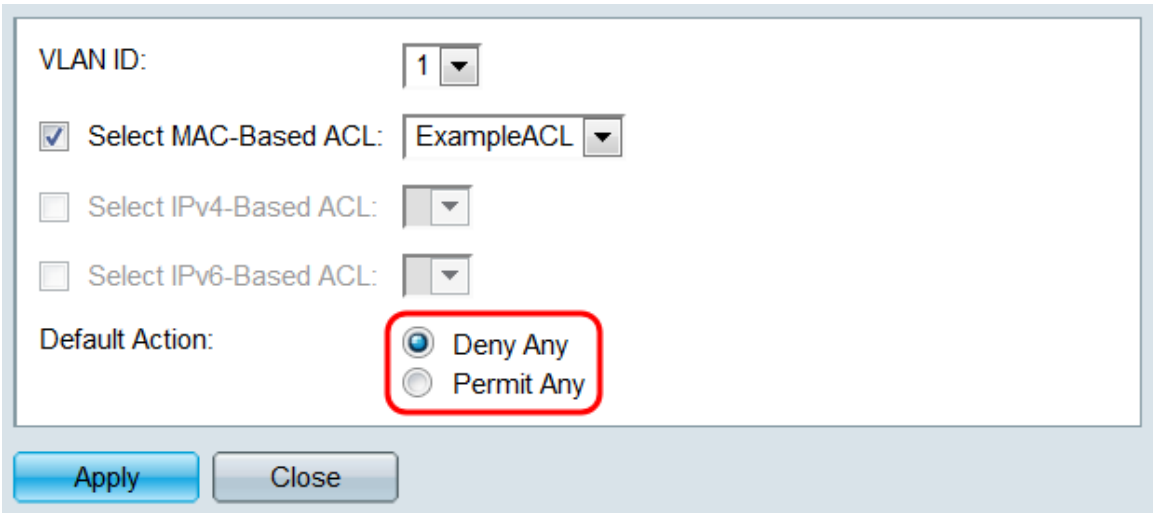


Etapa 4. Marque a caixa de seleção **Select MAC-Based ACL** e use a lista suspensa para selecionar uma ACL para mapear para a VLAN especificada.

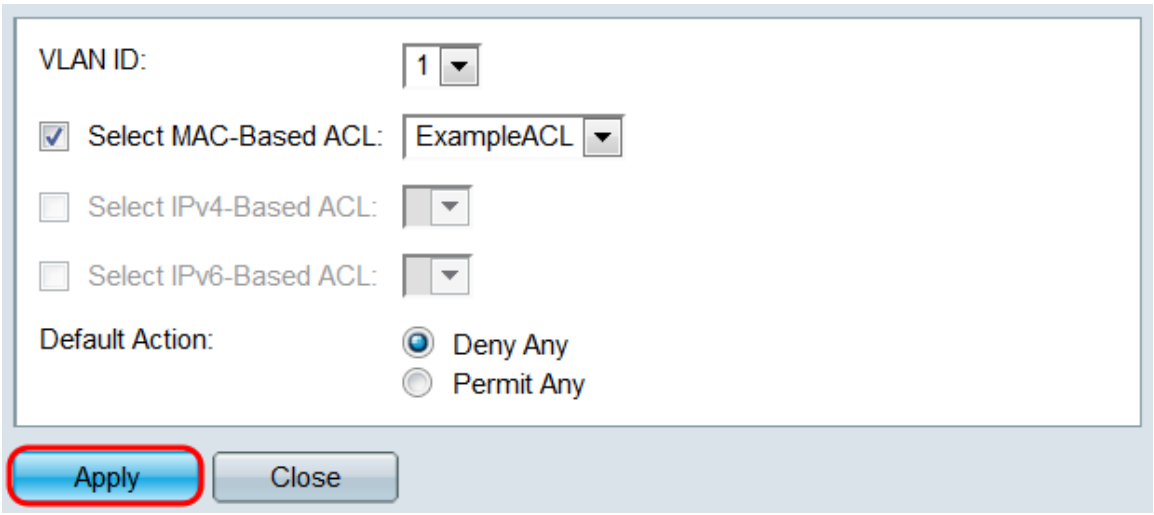


Note: Você não pode vincular uma ACL baseada em MAC que usa um ID de VLAN como parte de seus critérios a uma VLAN. Além disso, uma ACL com um intervalo de tempo não pode ser vinculada a uma VLAN.

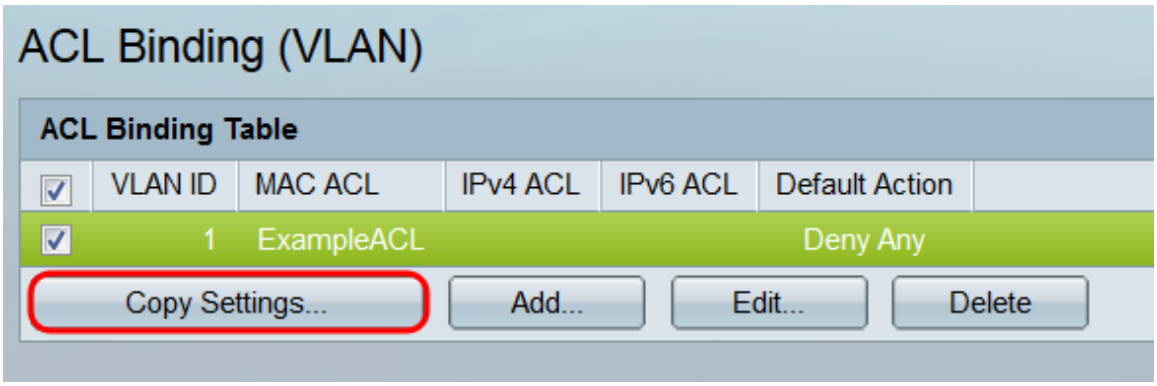
Etapa 5. No campo *Ação padrão*, selecione um botão de opção para determinar como os pacotes que não correspondem aos critérios da ACL serão tratados. O padrão é **Deny Any**, que descarta todos os pacotes que não correspondem aos critérios da ACL; **Permitir qualquer** encaminhará pacotes não correspondentes.



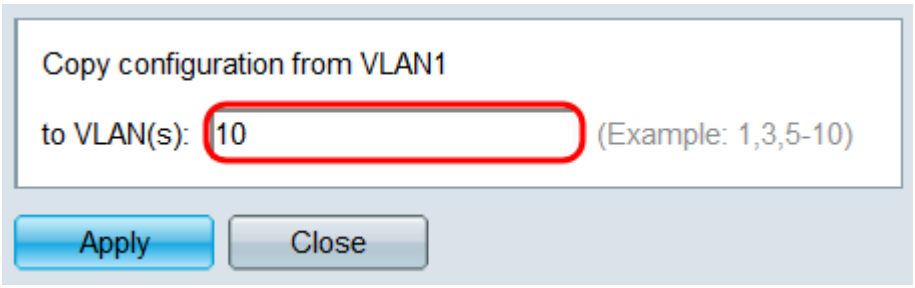
Etapa 6. Clique em Apply. A ACL é mapeada para a VLAN especificada. Você pode usar o campo *VLAN ID* para selecionar uma VLAN diferente para configurar ou clicar em **Fechar** para retornar à página *ACL Binding (VLAN)*.



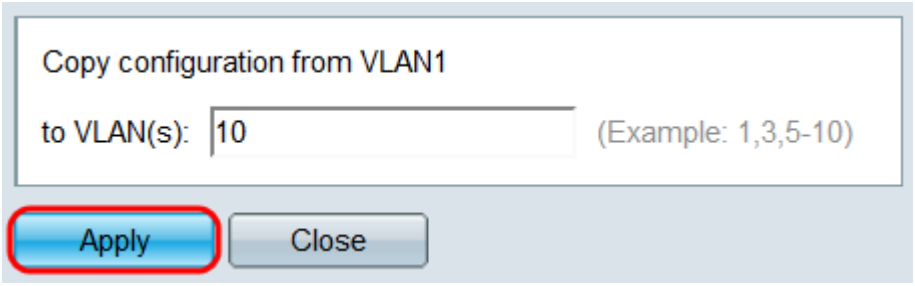
Passo 7. Para copiar rapidamente as configurações de uma VLAN para outras VLANs, marque a caixa de seleção da configuração da VLAN que deseja copiar e clique no botão **Copiar configurações...**. A janela *Copiar configurações* é aberta.



Etapa 8. No campo de texto, digite a ID da VLAN ou as IDs da VLAN para as quais deseja copiar as configurações. As IDs podem ser separadas por vírgulas ou um intervalo pode ser especificado.



Etapa 9. Clique em Apply. As configurações são copiadas.



Etapa 10. Se quiser limpar as configurações de uma VLAN, marque a caixa de seleção e clique em **Excluir**. Observe que várias VLANs podem ser selecionadas e limpas simultaneamente.