Creating a MAC-Based ACL on the SG350XG and SG550XG

Objective

An access control list (ACL) is a set of rules that can be created to manipulate packets depending on if they meet certain criteria. These criteria can be source or destination addresses, header fields, and other various components of a packet. If a packet matches an ACL's specified criteria, then it is either dropped or allowed to continue. A MAC-Based ACL uses rules that analyze a packet's Layer 2 header for these criteria, such as MAC addresses, VLAN IDs, and Ethertype values. Implementing a MAC-Based ACL allows you to control packets traveling across the switch at the Layer 2 level.

The objective of this document is to show you how to create and configure a MAC-Based ACL on the SG350XG and SG550XG switches.

Applicable Devices

- SG350XG
- SG550XG

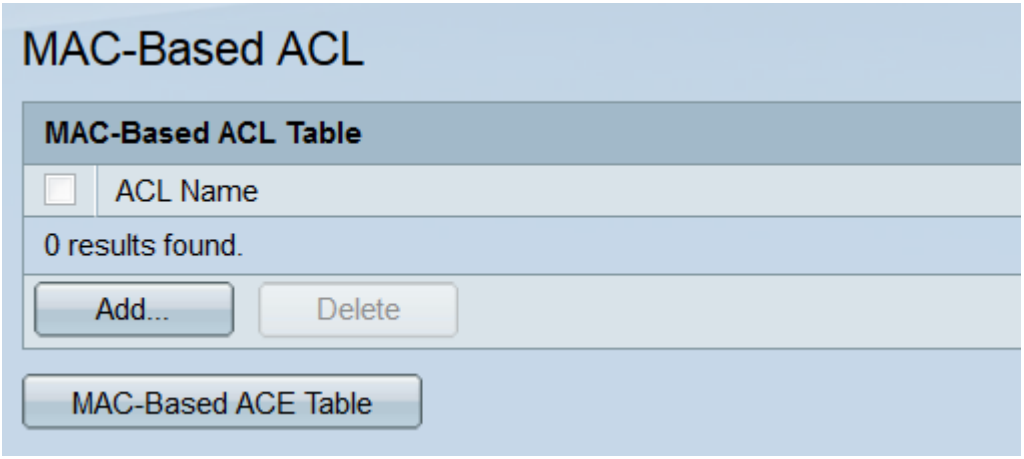
Software Version

- v2.0.0.73

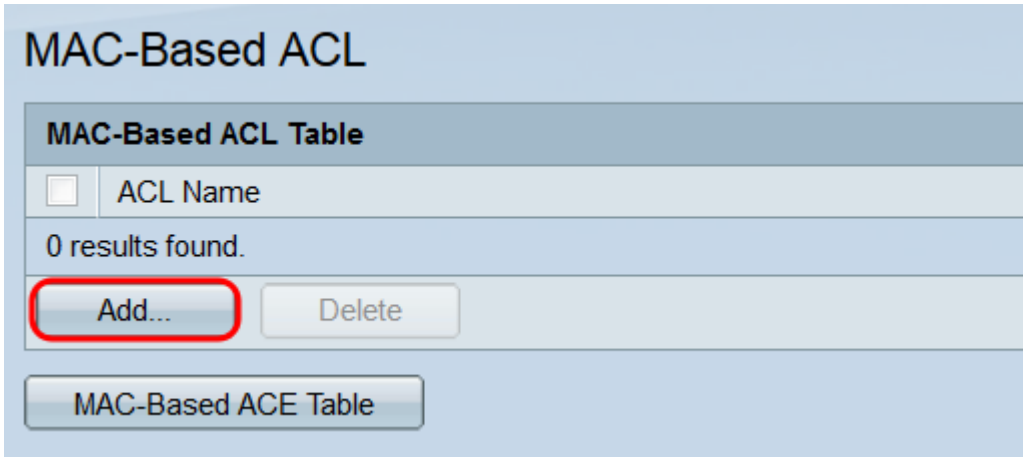
Configuring MAC-Based ACLs

Creating an ACL and Rules

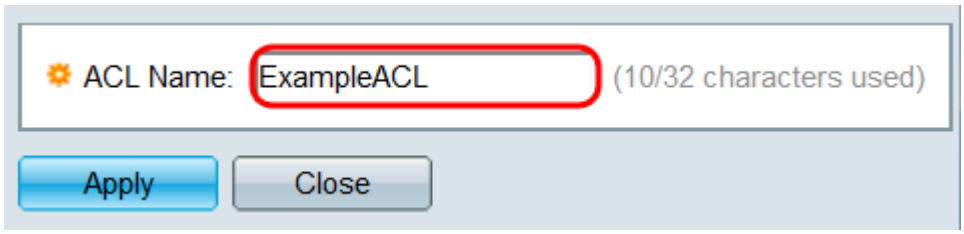
Step 1. Log in to the web configuration utility and choose **Access Control > MAC-Based ACL**. The *MAC-Based ACL* page opens.



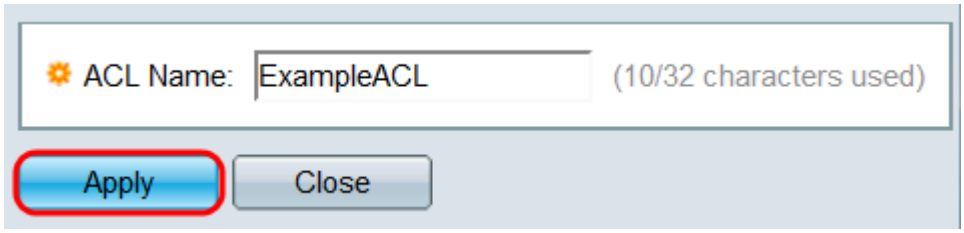
Step 2. The *MAC-Based ACL Table* will display all MAC-Based ACLs currently on the switch. To create a new ACL, click the **Add…** button. The *Add MAC-Based ACL* window will open.



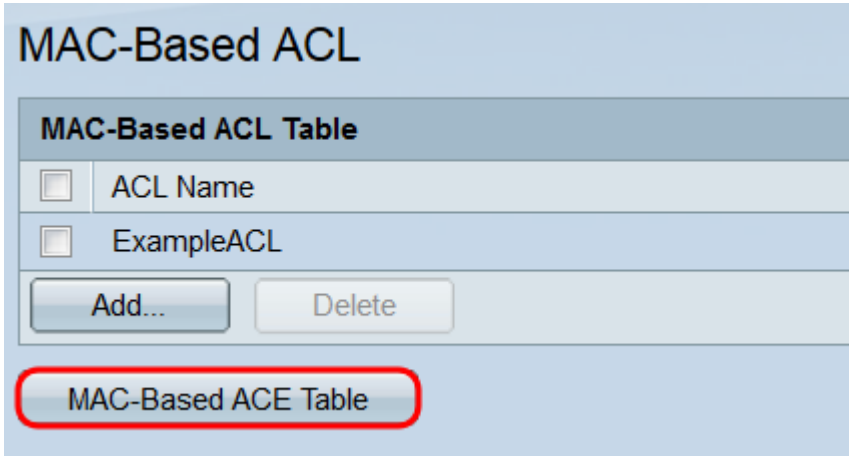
Step 3. In the *ACL Name* field, enter in the name for the new ACL. This name will not impact the function of the ACL, and is only for identification purposes.



Step 4. Click **Apply**. The new ACL will be added to the *MAC-Based ACL Table*. Click **Close** to return to the *MAC-Based ACL* page, or create another ACL by repeating the previous step.

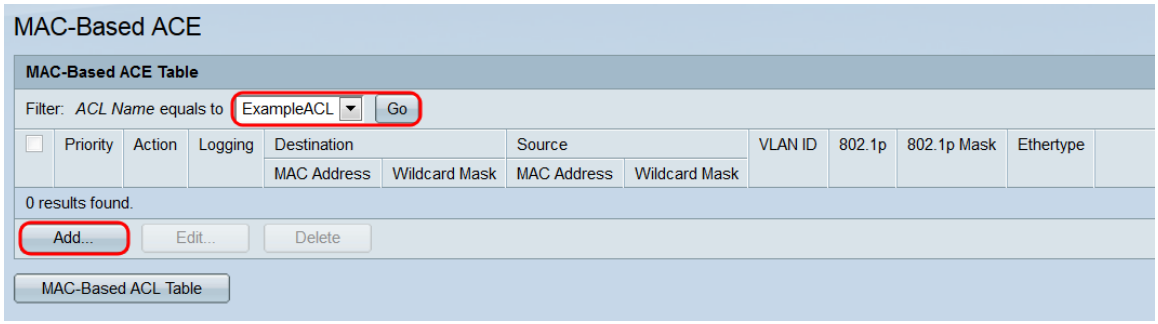


Step 5. Any newly created ACL will be empty; that is, it won't contain any rules to block or allow packets based on MAC addresses. To create these rules, an access control entry (ACE) must be added to the ACL. To do this, click the **MAC-Based ACE Table** button to go to the *MAC-Based ACE* page.

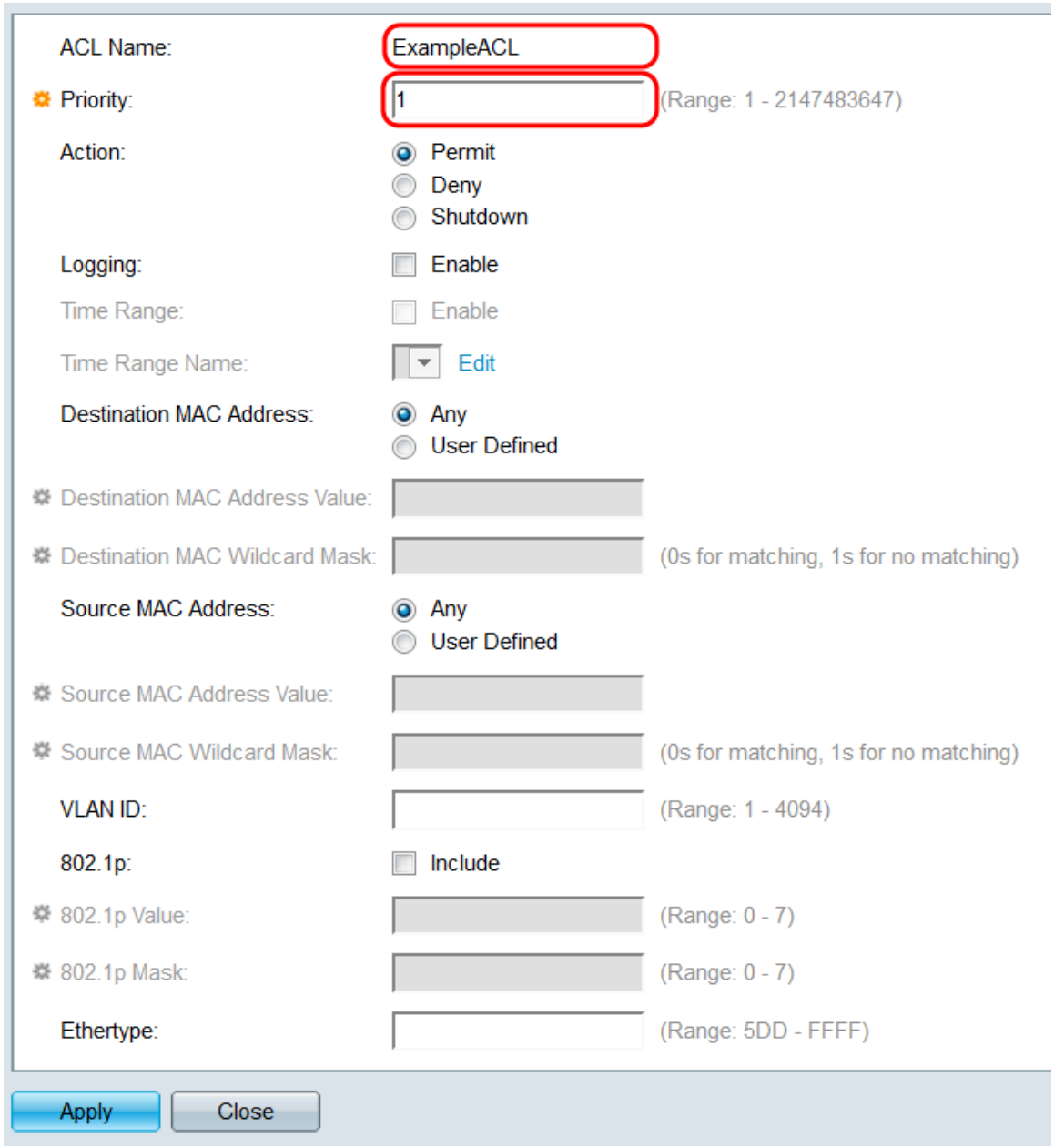


Step 6. On the *MAC-Based ACE* page, select the ACL that you want to add an ACE to via the drop-down list at the top of the *MAC-Based ACE Table* and click **Go**. The table displays any ACEs currently associated with the selected ACL. To add an ACE, click the **Add…**

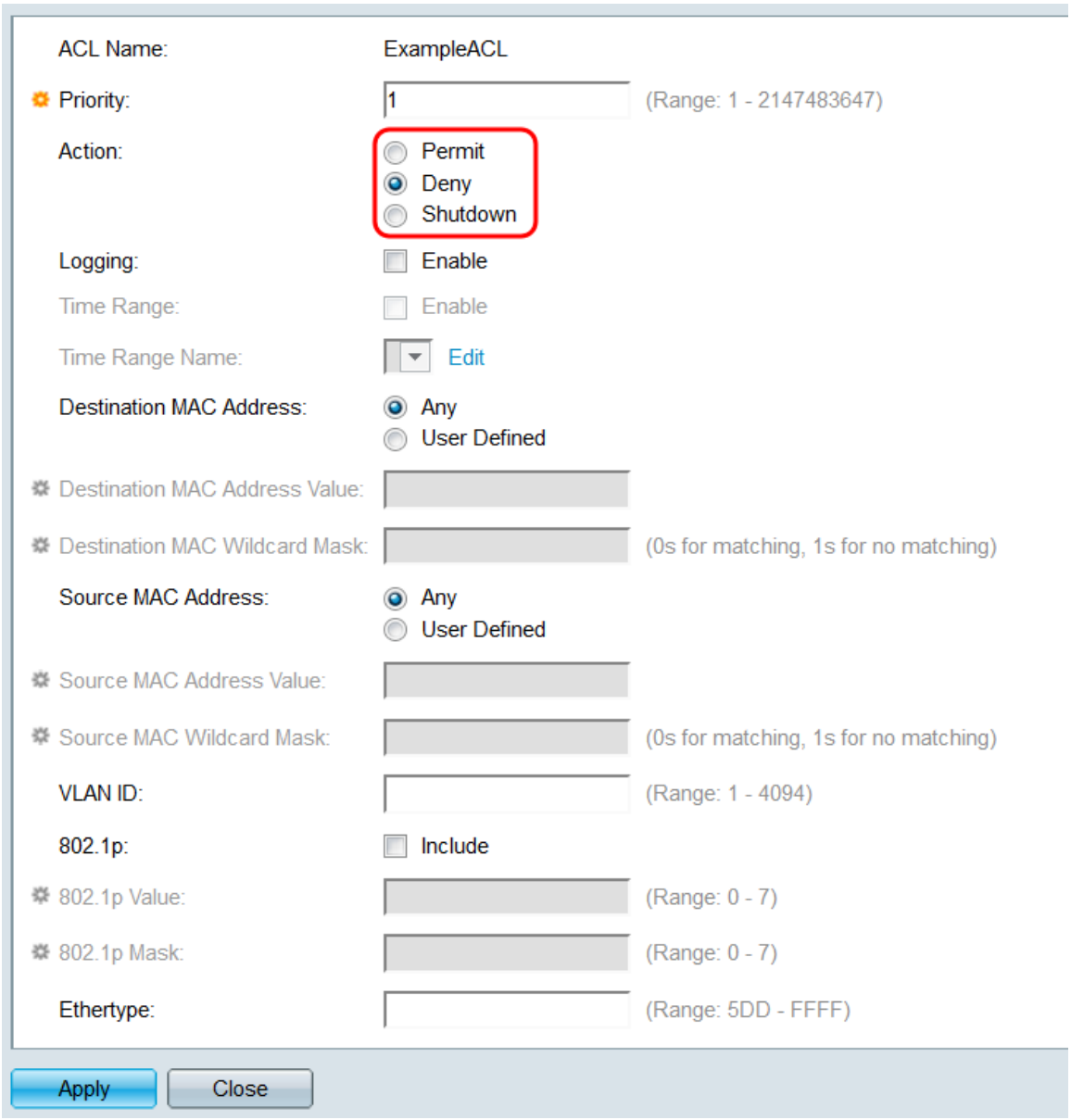
button. The *Add MAC-Based ACE* window will open.



Step 7. The *ACL Name* field will display the name of the ACL you are adding an ACE to. In the *Priority* field, enter in a priority number for the ACE. The higher an ACE's priority, the sooner it will be processed. The range is from 1 – 2147483647, with 1 being the highest priority.



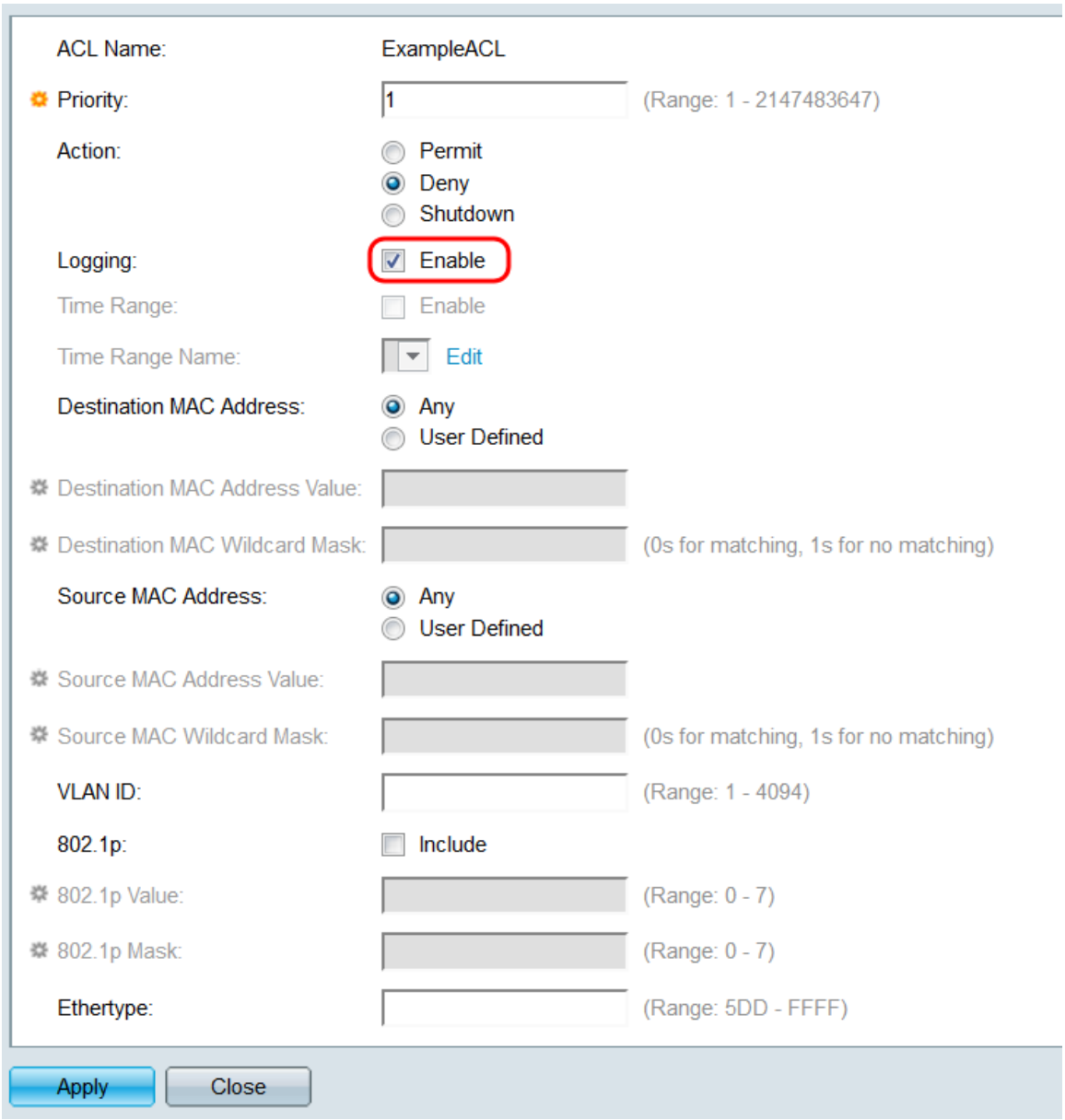
Step 8. In the *Action* field, select a radio button to determine what will happen when the ACE's criteria are met.



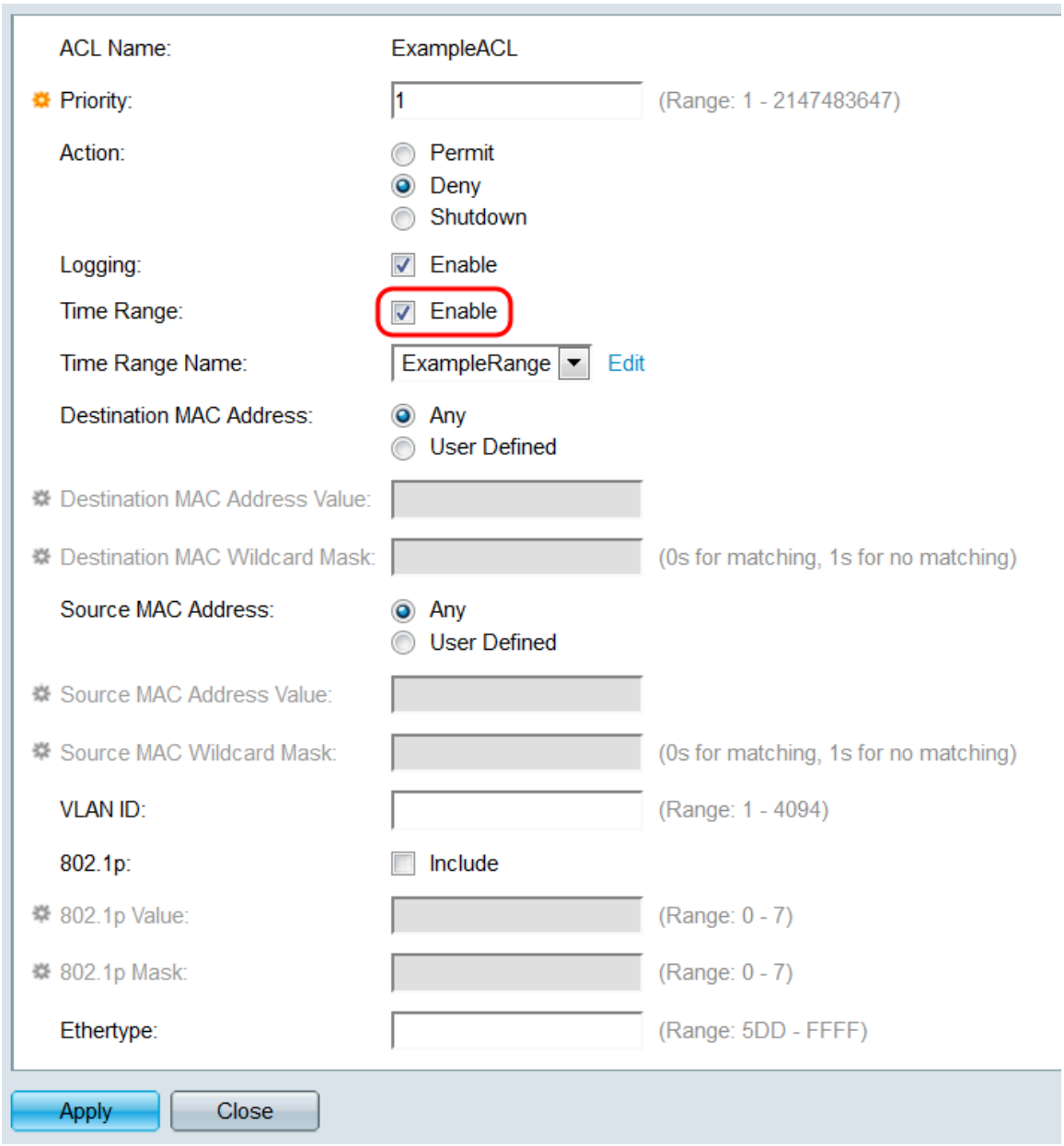
The options are:

- Permit – Forward packets that meet the criteria.
- Deny – Drop packets that meet the criteria.
- Shutdown – Drop packets that meet the criteria, then disable the port.

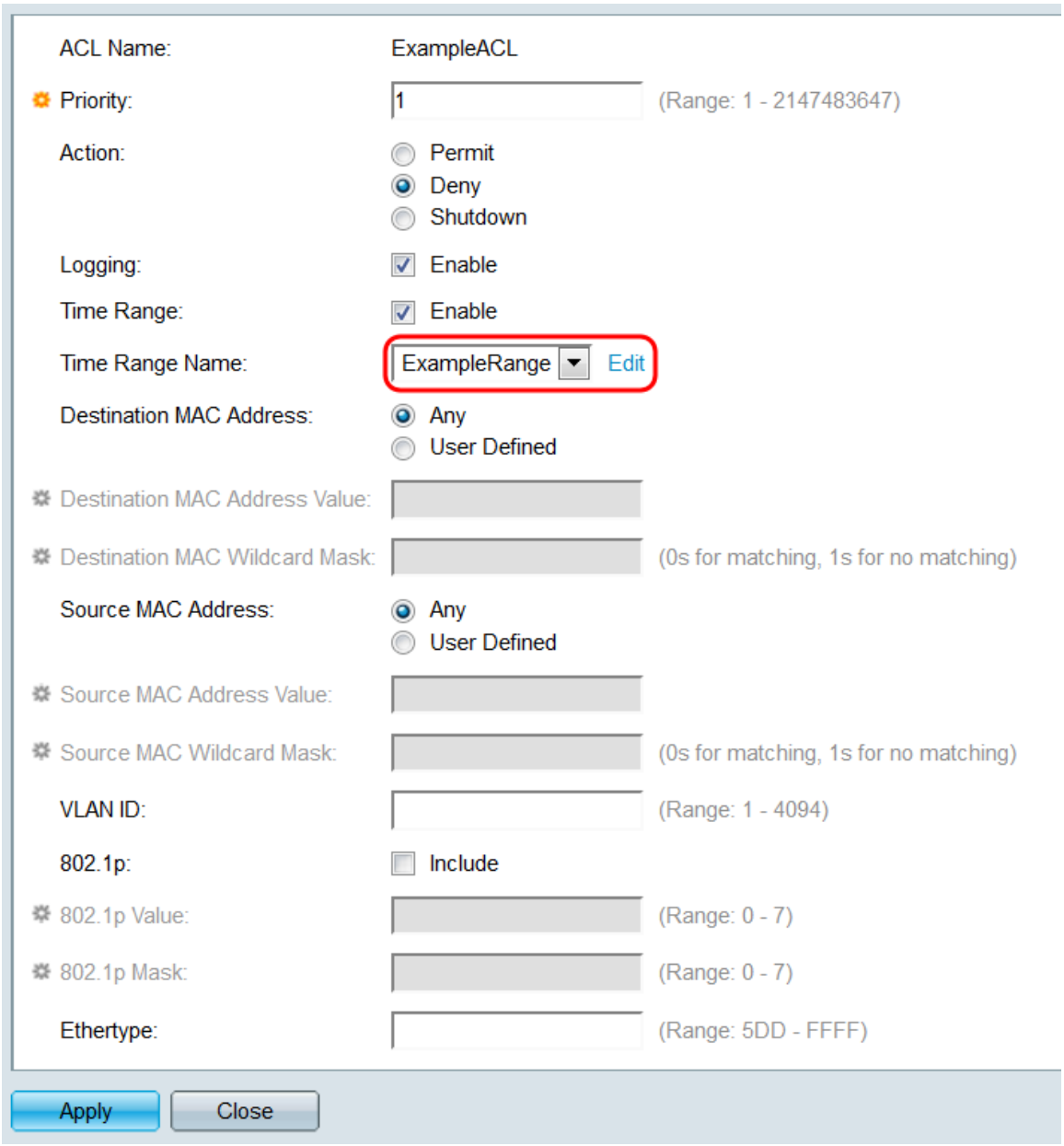
Step 9. In the *Logging* field, check the **Enable** checkbox to enable logging ACL flows that match the ACE rule. If you are using the Basic display mode, skip to Step 12. The display mode can be changed via the drop-down list in the top right corner of the web utility.



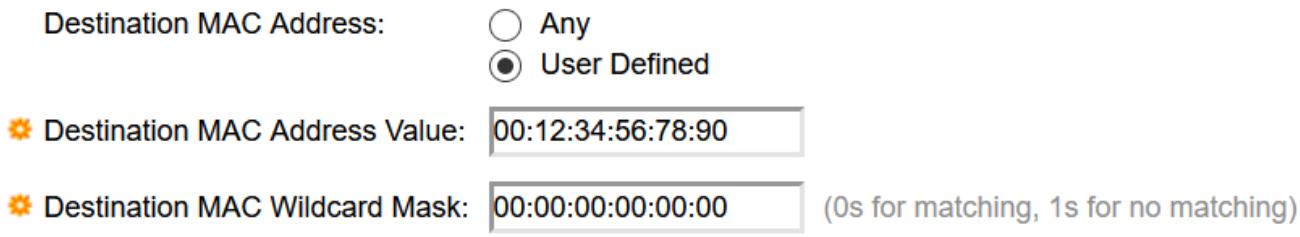
Step 10. In the *Time Range* field, check the **Enable** checkbox to have the ACE only be active during a specified time range. If there are no existing time ranges configured on the switch, this field will be unavailable.



Step 11. If you have enabled a time range for this ACE, the *Time Range Name* field will be available. Use the drop-down list to select a time range already configured on the switch to apply to the ACE. If no time ranges exist on the switch, this field will be unavailable; click the **Edit** link to go to the *Time Range* page to create or modify time ranges. For more information, please refer to the article *Setting Up a Time Range on the SG350XG and SG550XG*.



Step 12. In the *Destination MAC Address* field, select a radio button to determine what destination MAC addresses will constitute a match. Select **Any** to have any destination address be a match, or **User Defined** to specify an address or range of addresses.

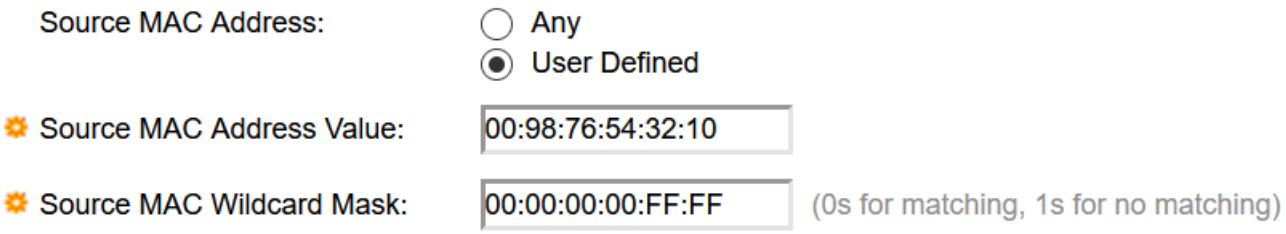


If you selected **User Defined**, fill out the following fields:

- Destination MAC Address Value – Enter the destination MAC address. If a packet contains this destination address, the ACE will consider it a match.
- Destination MAC Wildcard Mask – Enter a mask to define a range of addresses. Setting a bit as 1 will cause the corresponding bit in the MAC address to be ignored, and 0's will be matching bits.

Note : Given a mask of 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there's 0 and don't match on the bits where there are 1's). You need to translate the 1's to a hexadecimal value and you write 0 for every four zeros. In this example since 1111 1111 = FF, the mask would be written: as 00:00:00:00:00:FF.

Step 13. In the *Source MAC Address* field, select a radio button to determine what source MAC addresses will constitute a match. Select **Any** to have any source address be a match, or **User Defined** to specify an address or range of addresses.



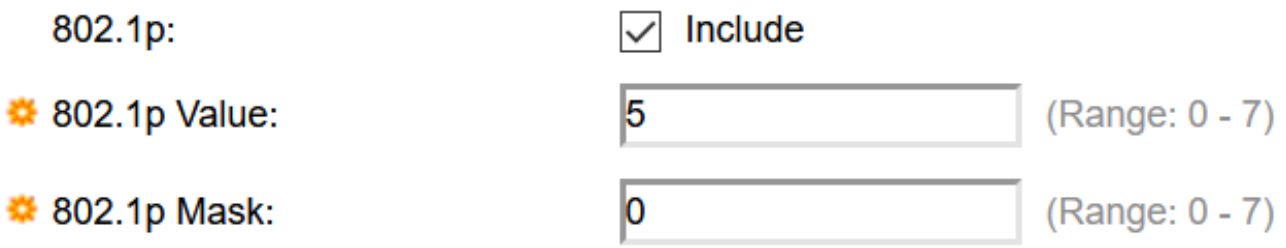
If you selected **User Defined**, fill out the following fields:

- Source MAC Address Value – Enter the source MAC address. If a packet contains this source address, the ACE will consider it a match.
- Source MAC Wildcard Mask – Enter a mask to define a range of addresses. Setting a bit as 1 will cause the corresponding bit in the MAC address to be ignored, and 0's will be matching bits (e.g. 00:00:00:00:00:11).

Note : Given a mask of 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there's 0 and don't match on the bits where there are 1's). You need to translate the 1's to a hexadecimal value and you write 0 for every four zeros. In this example since 1111 1111 = FF, the mask would be written: as 00:00:00:00:00:FF.

Step 14. In the *VLAN ID* field, enter a VLAN ID from 1 – 4094. If a packet contains this VLAN ID, the ACE will consider it a match. This field is not required; leaving it blank will cause the ACE to not consider VLAN IDs when examining packets.

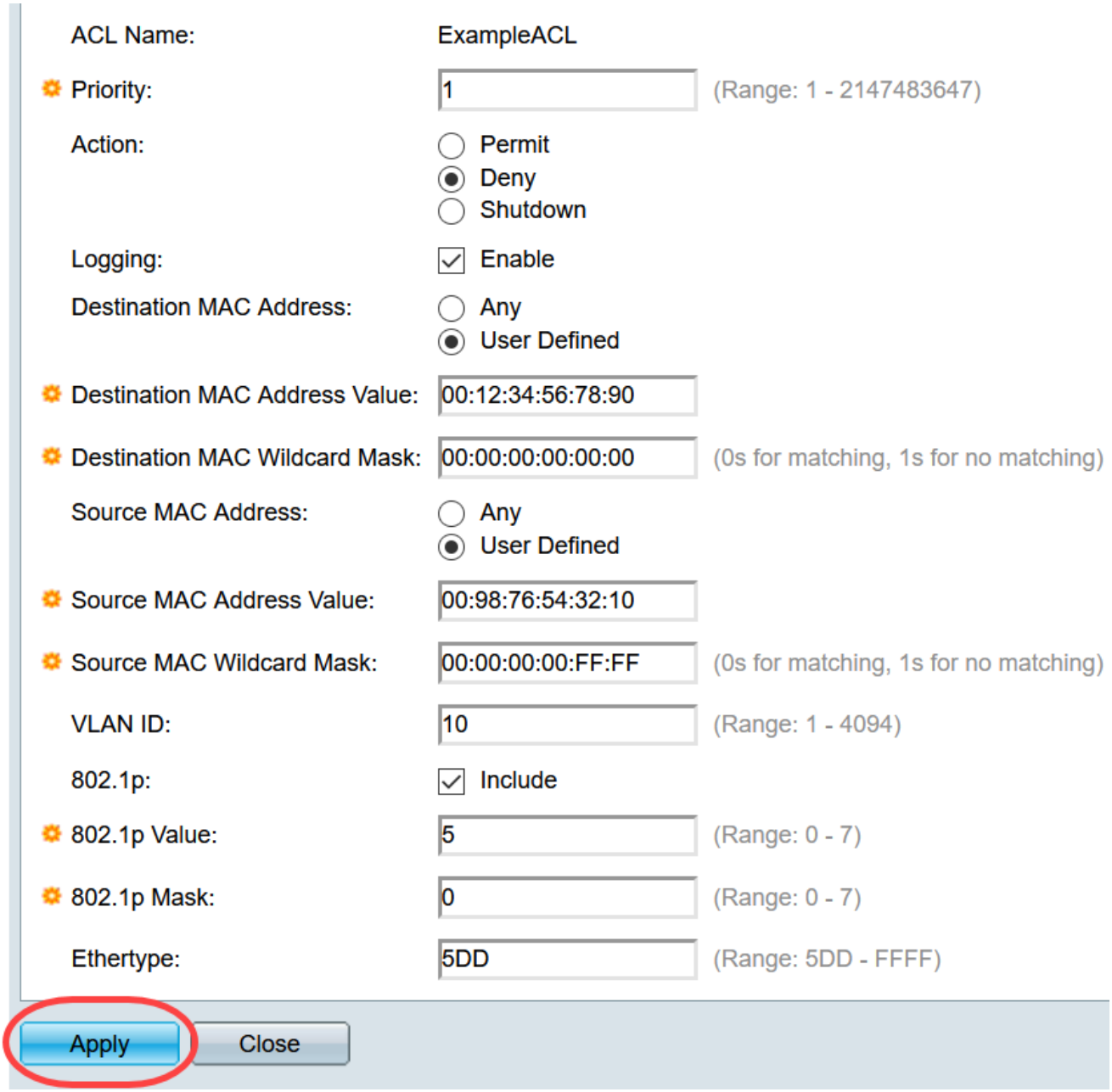
Step 15. In the *802.1p* field, check the **Include** checkbox to have the ACE include 802.1p criteria. If you included 802.1p criteria, enter an 802.1p value and mask in the *802.1p Value* and *802.1p Mask* fields, respectively. The range for both fields is 0 – 7. If a packet contains the corresponding 802.1p value and fits the mask, the ACE will consider it a match.



Step 16. In the *Ethertype* field, enter an Ethertype value that will be compared against

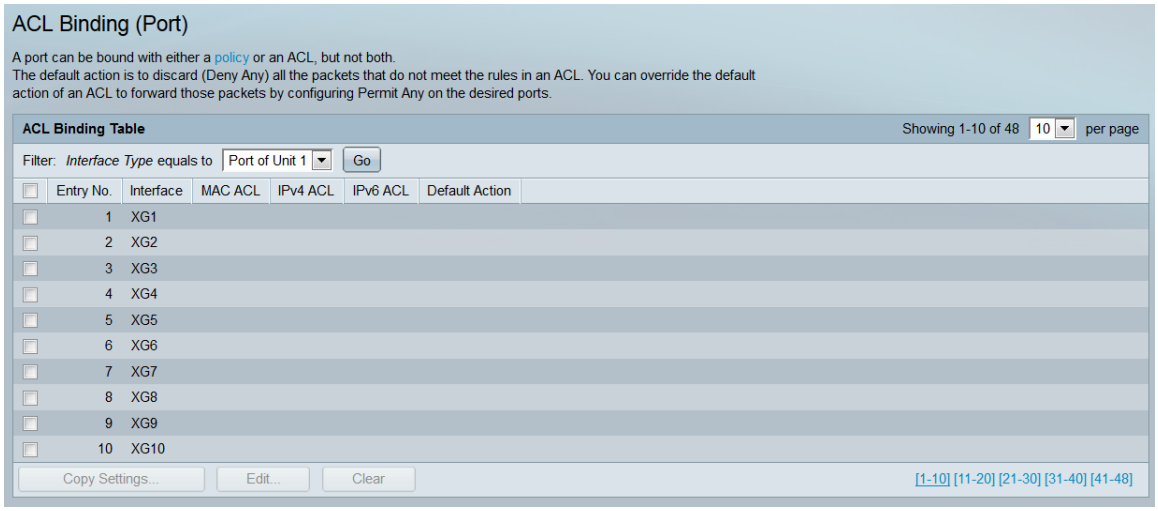
incoming packets. Ethertype is a two-octet field in a frame that indicates which protocol is encapsulated in the packet. The range is 5DD- FFFF. If a packet contains the specified Ethertype value, the ACE will consider it a match. A list of Ethertype values can be found on this IEEE standards page.

Step 17. Click **Apply**. The ACE will be added to the specified ACL. Click **Close** to return to the *MAC-Based ACE* page.

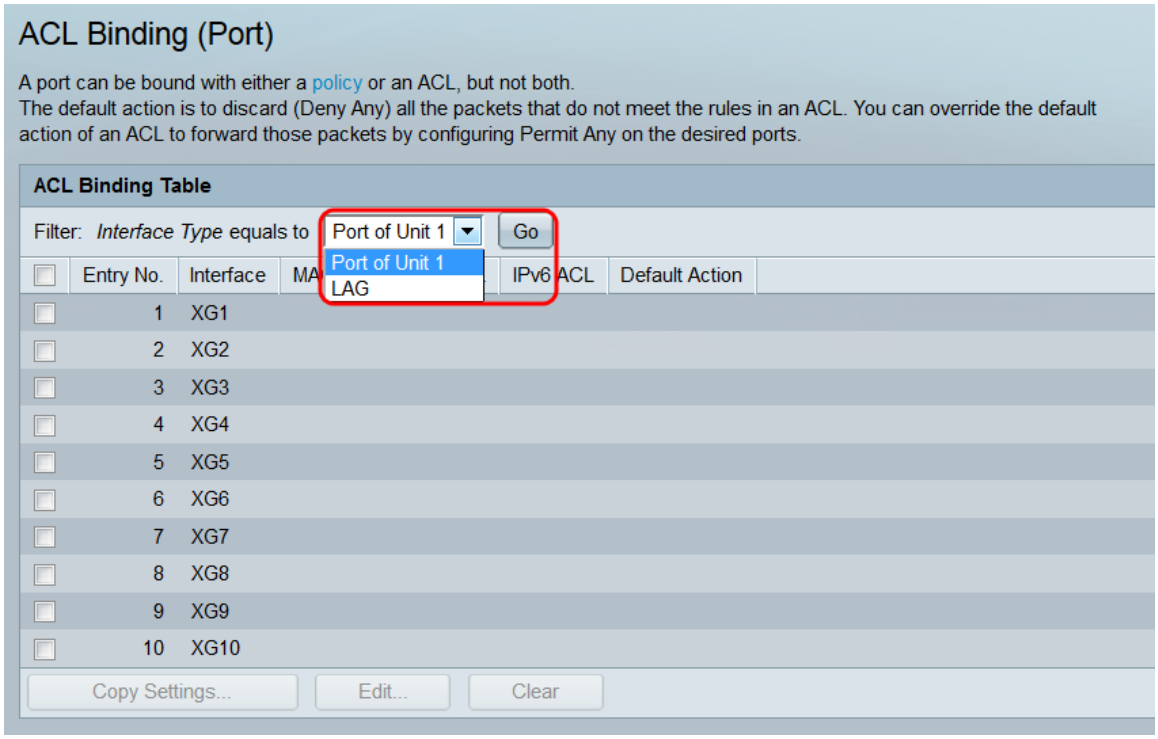


Mapping a MAC-Based ACL to Ports

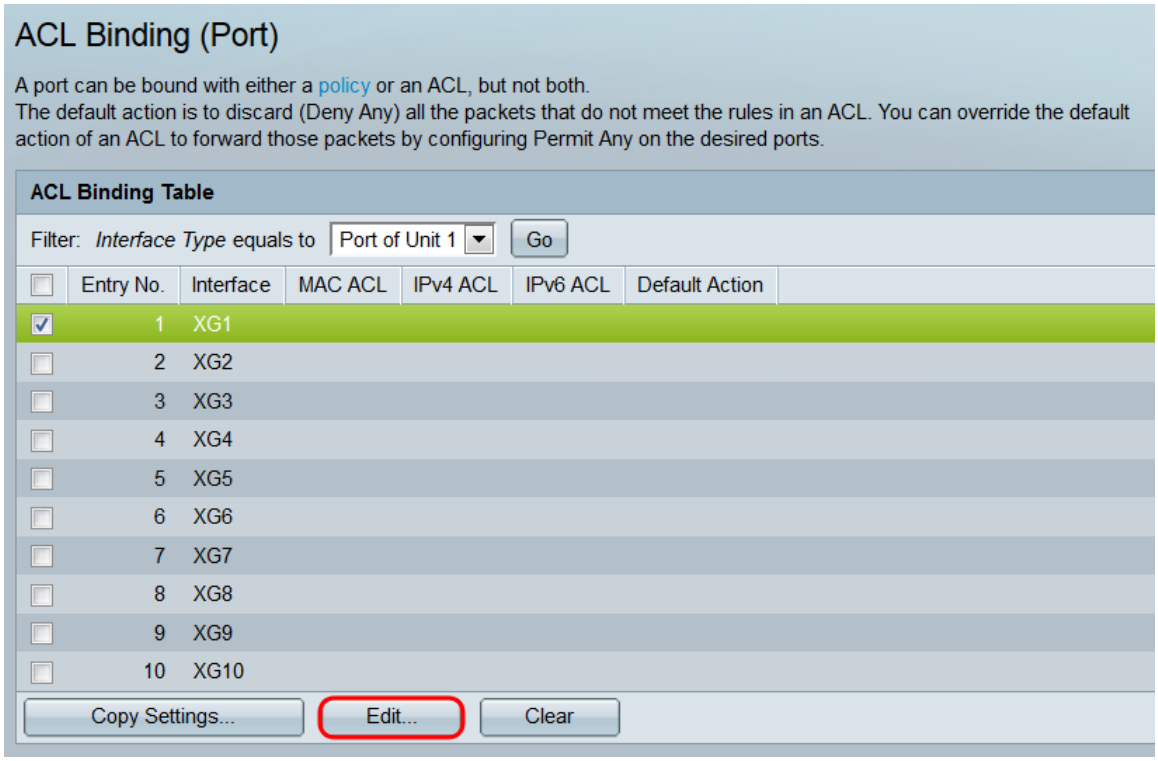
Step 1. An ACL can be mapped to either ports or VLANs. To map a MAC-Based ACL to a port or ports, navigate to **Access Control > ACL Binding (Port)**. The *ACL Binding (Port)* page opens.



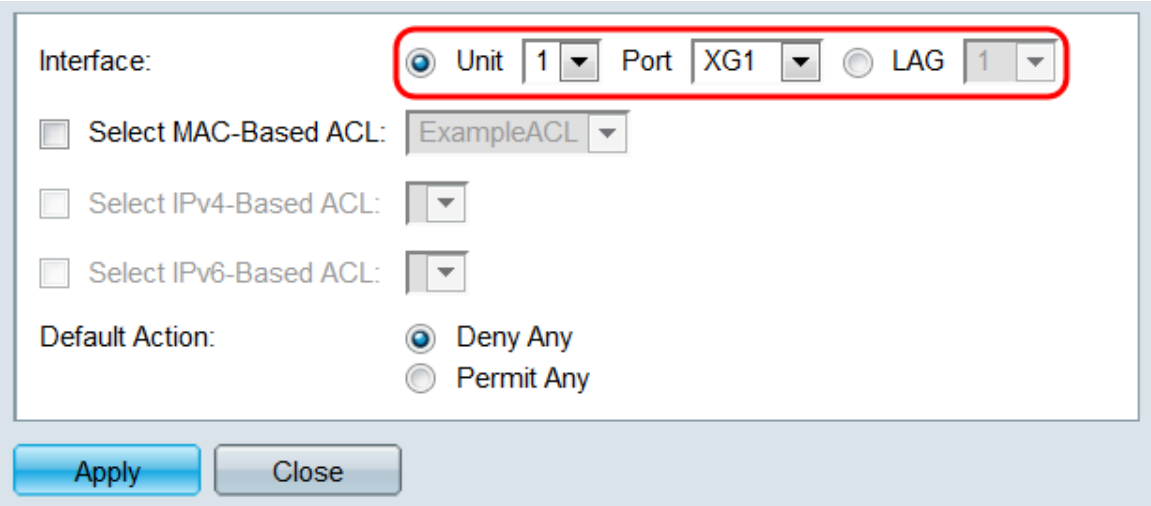
Step 2. In the drop-down list at the top of the *ACL Binding Table*, select either ports or LAG (link aggregation group) as an interface type. If the switch is part of a stack, ports from other units can be selected. Click **Go** to display a list of the specified interface type.



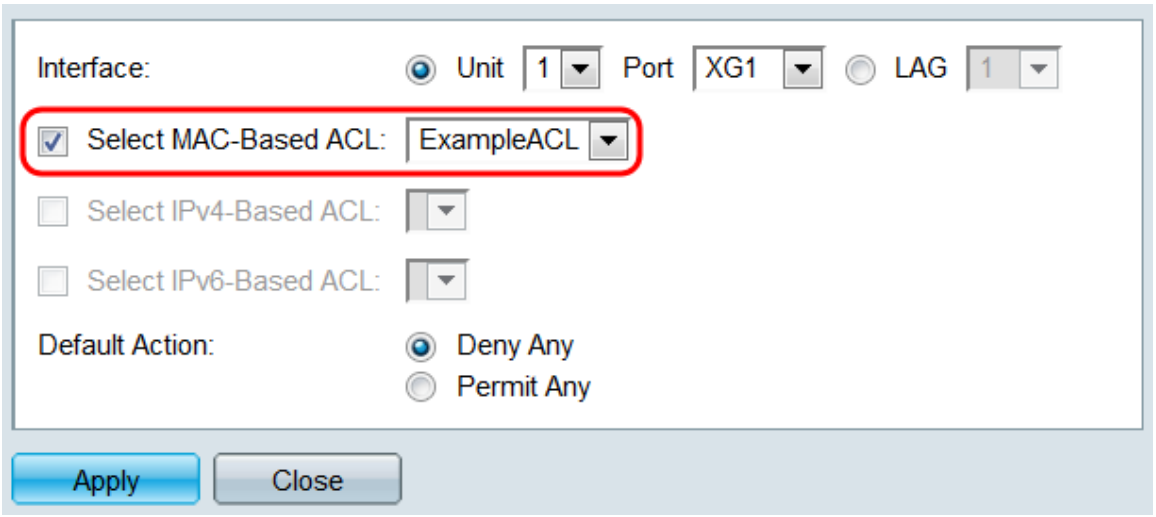
Step 3. Select an interface's checkbox, then click the **Edit…** button. The *Edit ACL Binding* window opens.



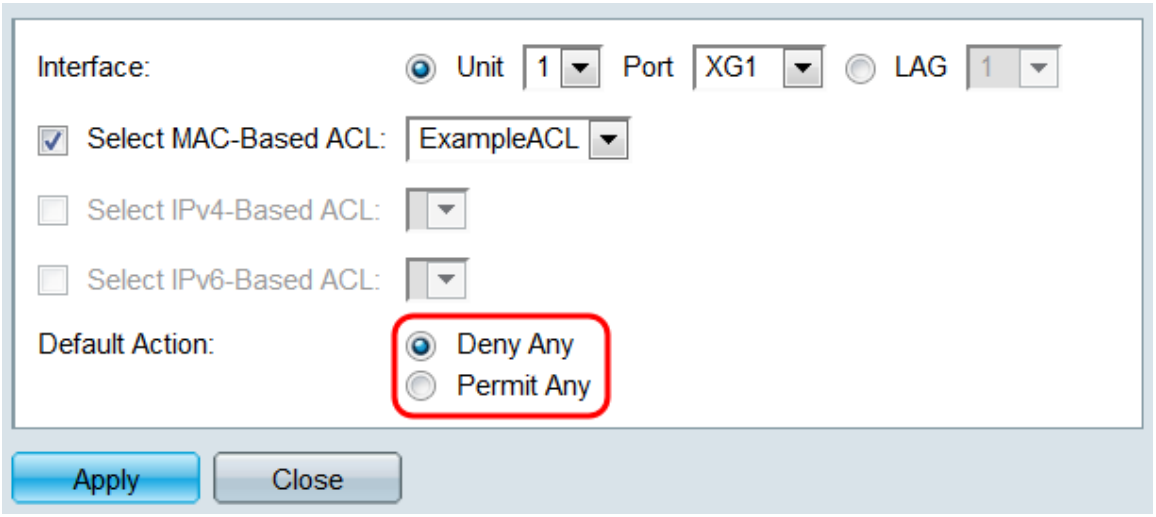
Step 4. The *Interface* field displays the port or LAG currently being configured. It will automatically show the interface selected in the *ACL Binding Table*. This field can be used to quickly switch between different interfaces without returning to the *ACL Binding (Port)* page.



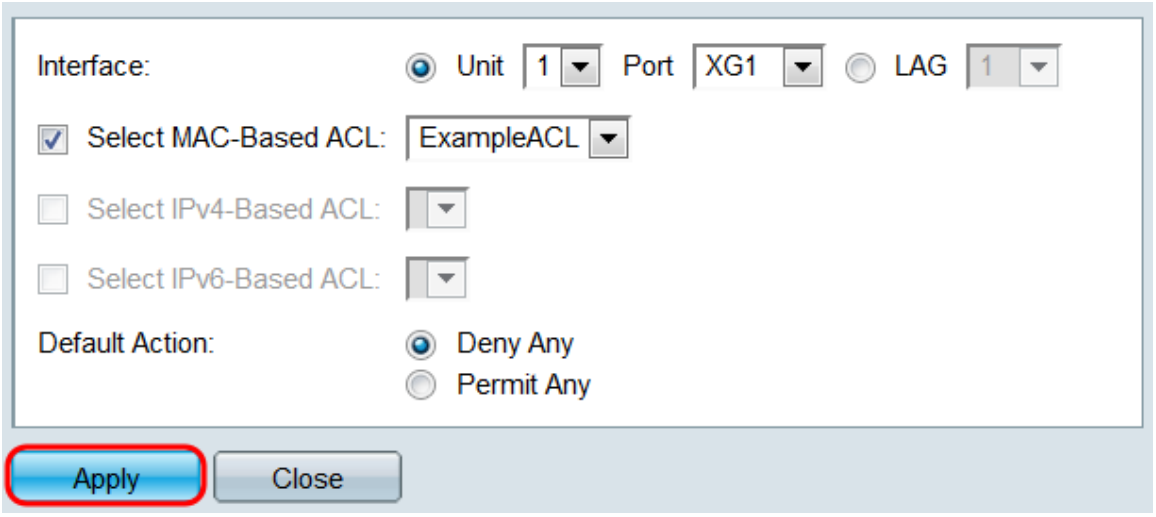
Step 5. Check the **Select MAC-Based ACL** checkbox, and use the drop-down list to select an ACL to map to the specified interface.



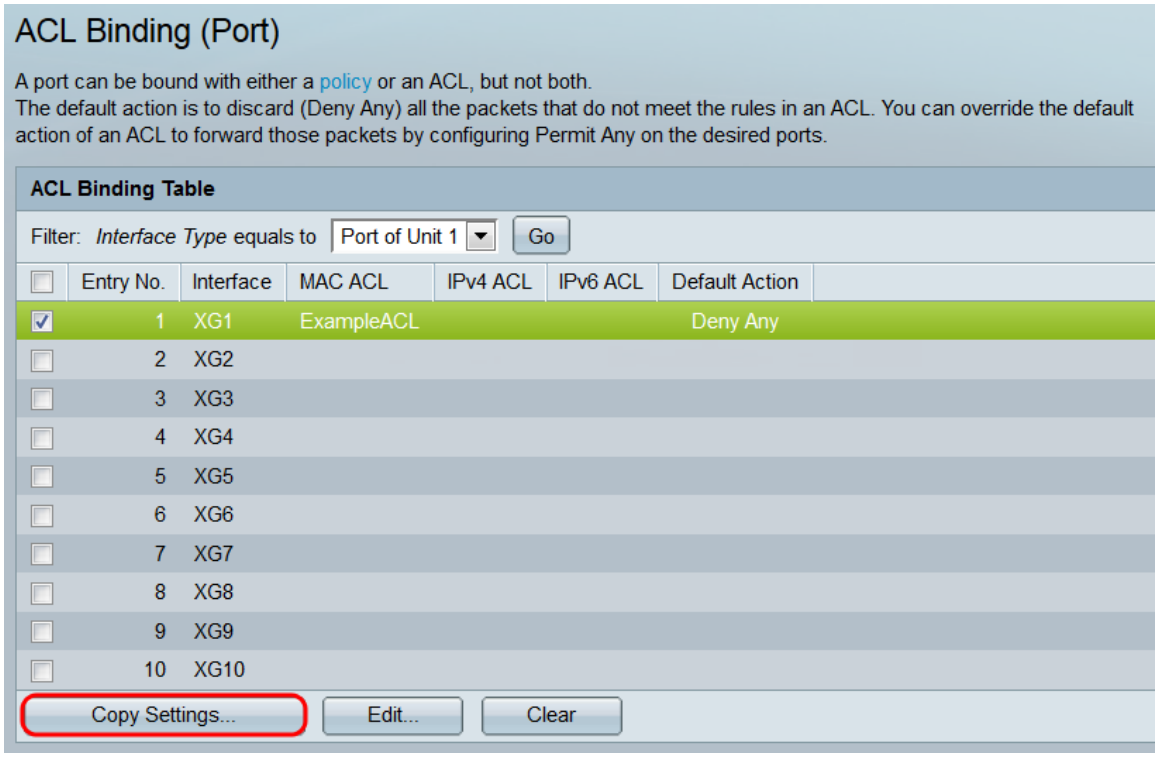
Step 6. In the *Default Action* field, select a radio button to determine how packets that don't match the ACL's criteria will be handled. The default is **Deny Any**, which drops any packets that don't match the ACL's criteria; **Permit Any** will forward non-matching packets instead.



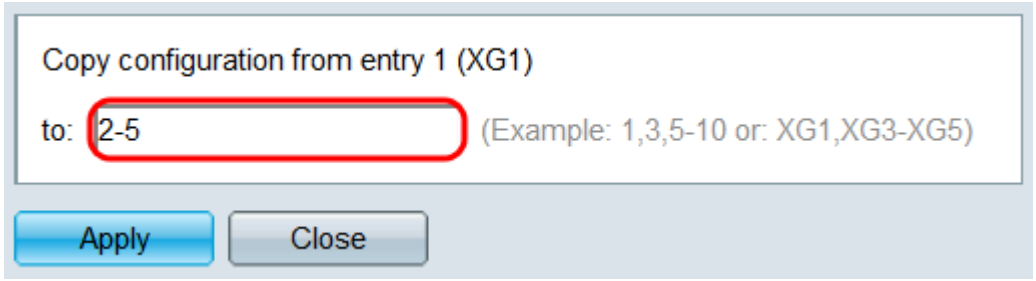
Step 7. Click **Apply**. The ACL is mapped to the specified interface. You can use the *Interface* field to select a different interface to configure, or click **Close** to return to the *ACL Binding (Port)* page.



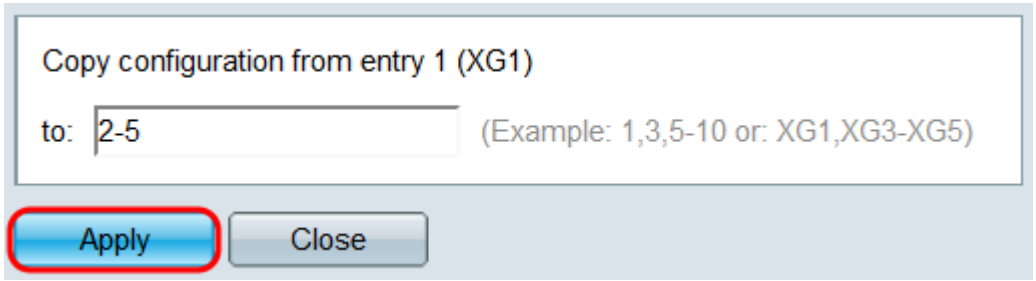
Step 8. To quickly copy an interface's settings to other interfaces, select the checkbox of the interface you want to copy, then click the **Copy Settings…** button. The *Copy Settings* window opens.



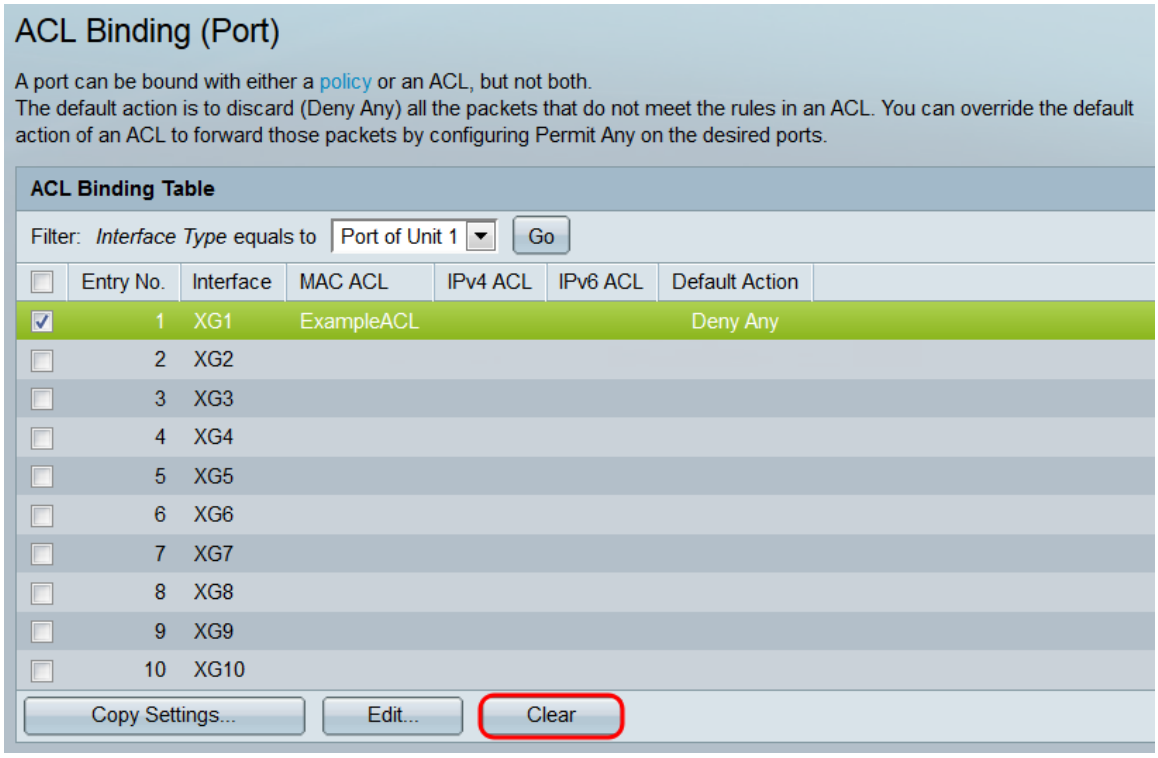
Step 9. In the text field, enter the interface or interfaces that you want to copy settings to. The interfaces can be separated by commas, or a range can be specified.



Step 10. Click **Apply**. The settings are copied.

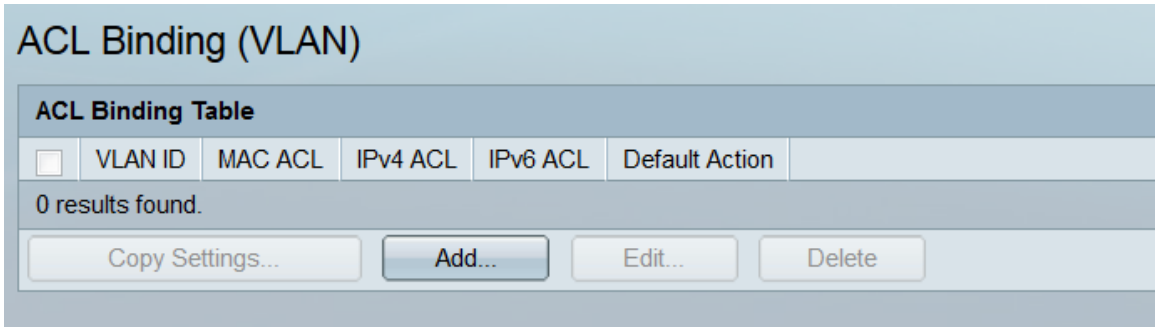


Step 11. If you want to clear an interface's settings, select its checkbox and click **Clear**. Note that multiple interfaces can be selected and cleared simultaneously.

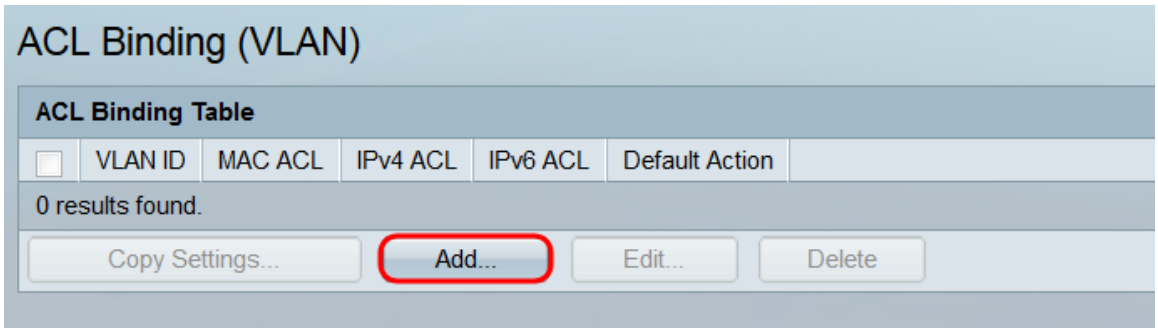


Mapping a MAC-Based ACL to VLANs

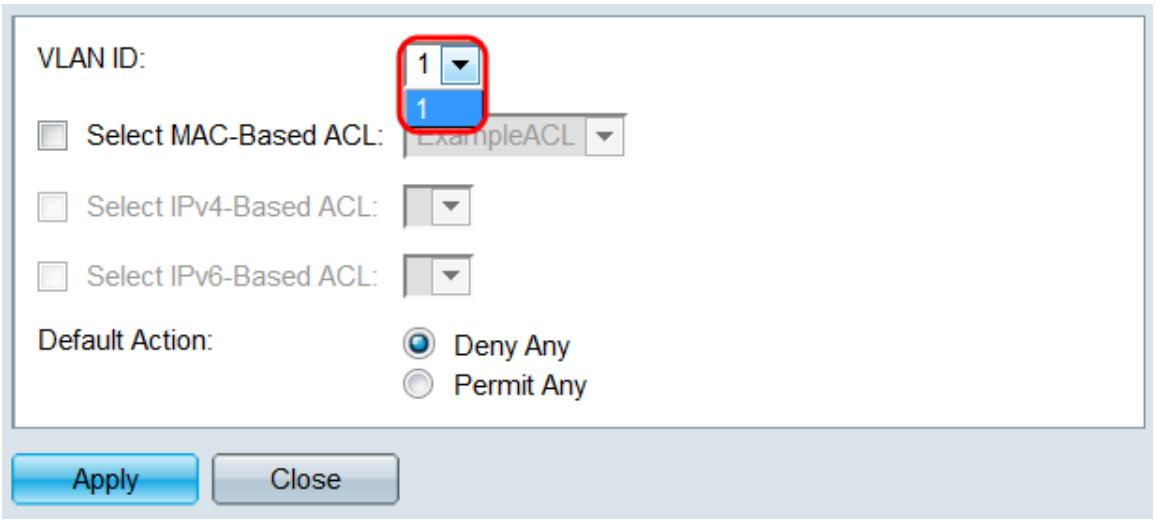
Step 1. An ACL can be mapped to either ports or VLANs. To map a MAC-Based ACL to a VLAN, navigate to **Access Control > ACL Binding (VLAN)**. The *ACL Binding (VLAN)* page opens.



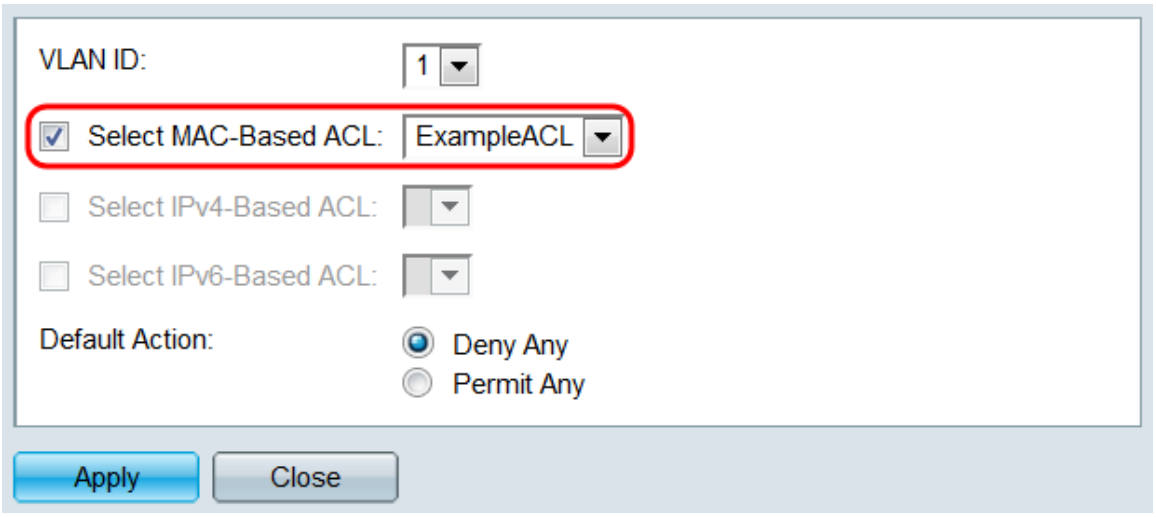
Step 2. The *ACL Binding Table* displays all ACLs currently mapped to VLANs. If no ACLs have been mapped, then the table is empty. To map an ACL to a VLAN, click the **Add…** button. The *Add ACL Binding* window opens.



Step 3. Select a VLAN to map an ACL to using the drop-down list in the *VLAN ID* field. This field can also be used to quickly switch between different VLANs without returning to the *ACL Binding (VLAN)* page.

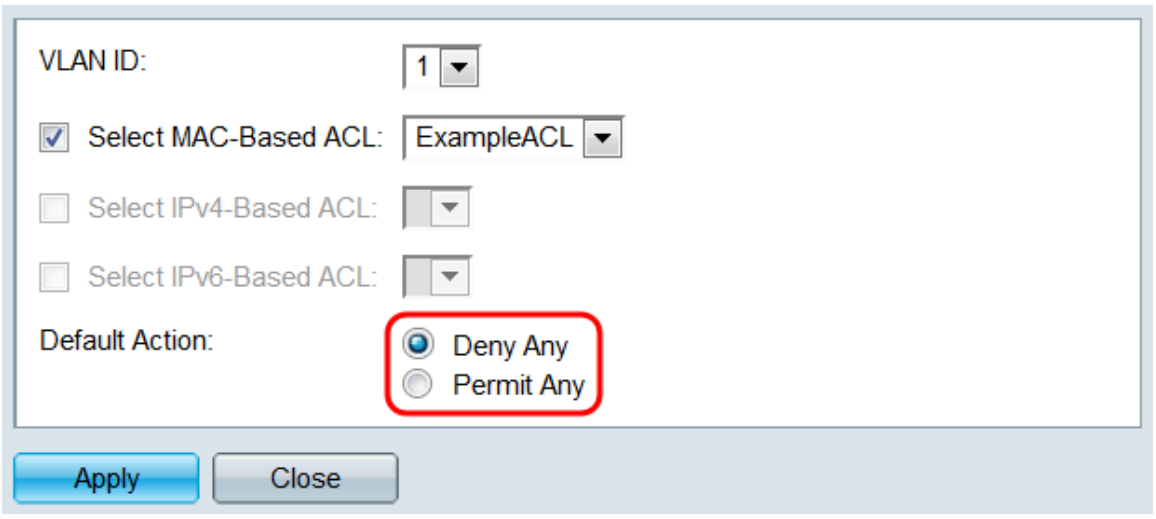


Step 4. Check the **Select MAC-Based ACL** checkbox, and use the drop-down list to select an ACL to map to the specified VLAN.



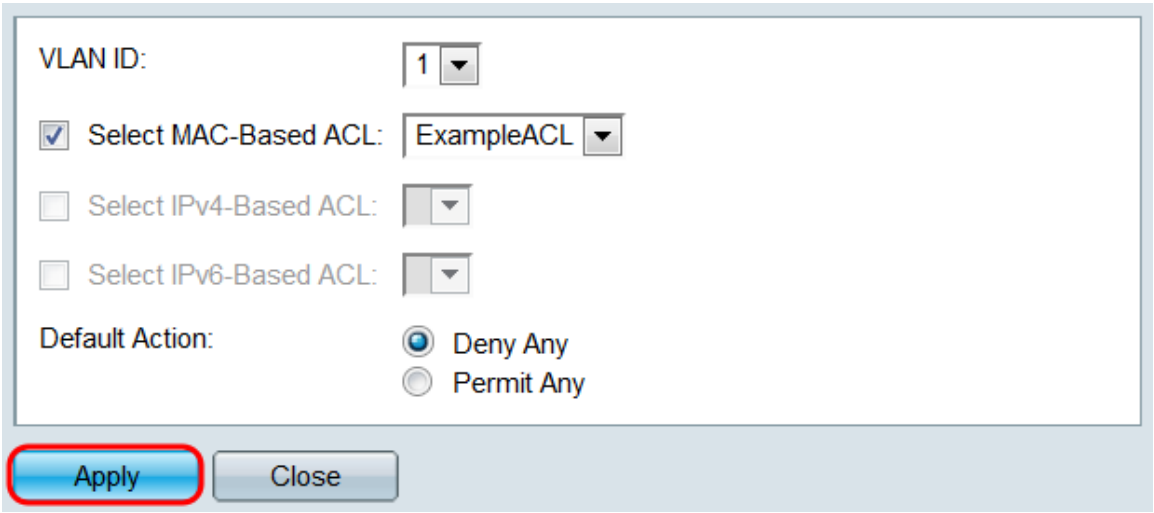
Note: You cannot bind a MAC-Based ACL that uses a VLAN ID as part of its criteria to a VLAN. In addition, an ACL with a time range cannot be bound to a VLAN.

Step 5. In the *Default Action* field, select a radio button to determine how packets that don't match the ACL's criteria will be handled. The default is **Deny Any**, which drops any packets that don't match the ACL's criteria; **Permit Any** will forward non-matching packets instead.

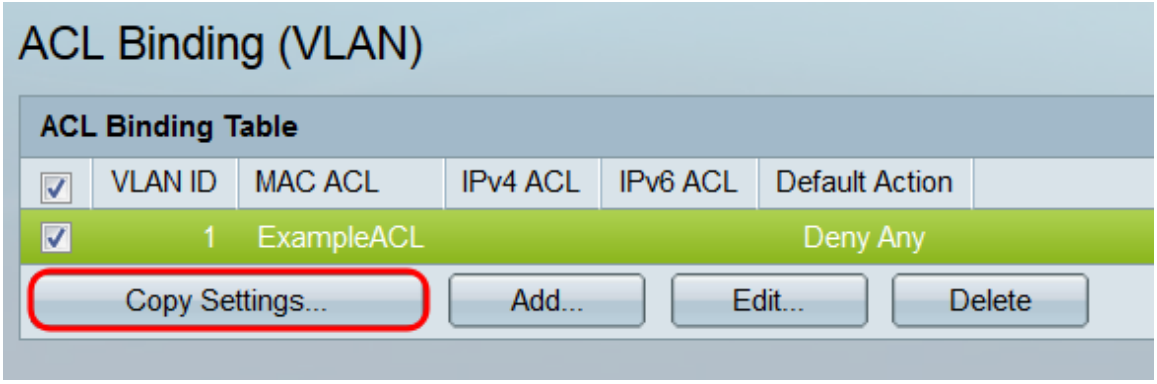


Step 6. Click **Apply**. The ACL is mapped to the specified VLAN. You can use the *VLAN ID*

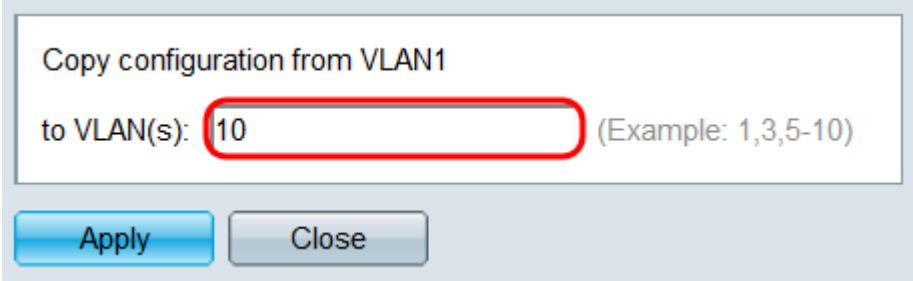
field to select a different VLAN to configure, or click **Close** to return to the *ACL Binding (VLAN)* page.



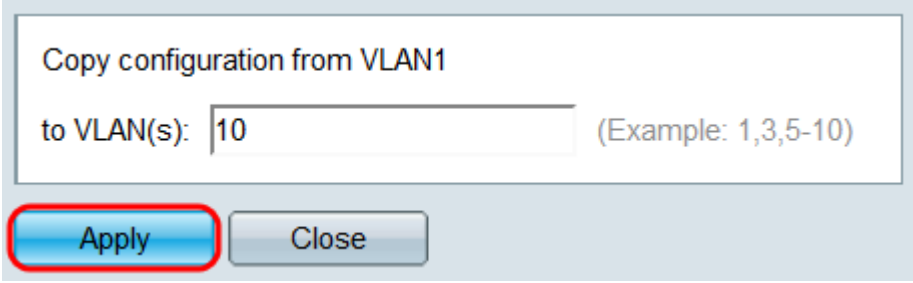
Step 7. To quickly copy a VLAN's settings to other VLANs, select the checkbox of the VLAN configuration you want to copy, then click the **Copy Settings…** button. The *Copy Settings* window opens.



Step 8. In the text field, enter the VLAN ID or VLAN IDs that you want to copy settings to. The IDs can be separated by commas, or a range can be specified.



Step 9. Click **Apply**. The settings are copied.



Step 10. If you want to clear a VLAN's settings, select its checkbox and click **Delete**. Note

that multiple VLANs can be selected and cleared simultaneously.