

MAC Based Access Control List (ACL) and Access Control Entry (ACE) Configuration on 300 Series Managed Switches

Objective

An Access Control List (ACL) is a security technology that is used to permit or deny network traffic flow. MAC-Based ACLs use Layer 2 information to permit or deny access to traffic. An Access Control Entry (ACE) contains the actual access rule criteria. Once the ACE is created, it is applied to an ACL. The 300 Series Managed Switches support a maximum of 512 ACLs and 512 ACEs.

This article explains how to create MAC Based ACLs and how to apply ACEs to the ACLs on the 300 Series Managed Switches.

Applicable Devices

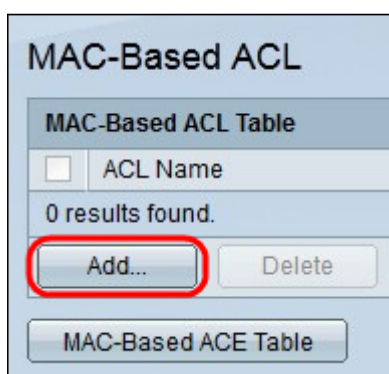
- SG/SF 300 Series Managed Switches

Software Version

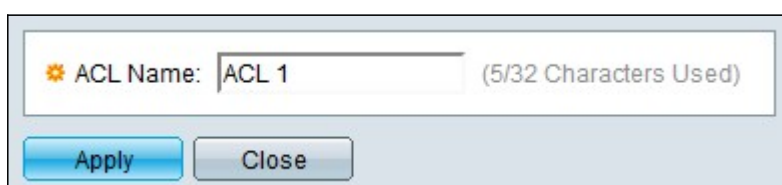
- 1.3.0.62

MAC-Based ACL

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

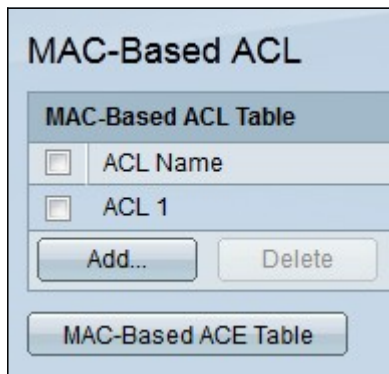


Step 2. Click **Add**. The *Add MAC-Based ACL* window appears.



Step 3. Enter a name for the ACL in the ACL Name field.

Step 4. Click **Apply**. The ACL is created.



The screenshot shows a web interface for configuring a MAC-Based ACL. At the top, the title is "MAC-Based ACL". Below it is a section titled "MAC-Based ACL Table". This section contains a table with two rows: the first row has a checkbox and the text "ACL Name", and the second row has a checkbox and the text "ACL 1". Below the table are two buttons: "Add..." and "Delete". At the bottom of the interface is a button labeled "MAC-Based ACE Table".

MAC-Based ACE

When a frame is received on a port, the switch processes the frame through the first ACL. If the frame matches an ACE filter of the first ACL, the ACE action takes place. If the frame matches none of the ACE filters, the next ACL is processed. If no match is found to any ACE in all relevant ACLs, the frame is dropped by default.

Note: This default action can be avoided by the creation of a low priority ACE that permits all traffic.

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

Step 2. From the ACL Name drop-down list, choose an ACL to apply a rule to.

Step 3. Click **Go**. The ACEs that are already configured for the ACL are displayed.

Step 4. Click **Add** to add a new rule to the ACL. The *Add MAC-Based ACE* window appears.

The ACL Name field displays the name of the ACL.

Step 5. Enter the priority value for the ACE in the Priority field. ACEs with a higher priority value are processed first. The value 1 is the highest priority.

Step 6. Click the radio button that corresponds to the desired action that is taken when a frame meets the required criteria of the ACE.

- Permit — The switch forwards packets that meet the required criteria of the ACE.
- Deny — The switch drops packets that do not meet the required criteria of the ACE.
- Shutdown — The switch drops packets that do not meet the required criteria of the ACE and disables the port where the packets were received.

Note: Disabled ports can be reactivated on the *Port Settings* page.

Step 7. Check the **Enable** check box in the Time Range field to allow a time range to be configured to the ACE. Time ranges are used to limit the amount of time an ACE is in effect.

Step 8. From the Time Range Name drop-down list, choose a time range to apply to the ACE.

Note: Click **Edit** to navigate to and create a time range on the *Time Range* page.

Step 9. Click the radio button that corresponds to the desired criteria of the ACE in the

Destination MAC Address field.

Step 10. Click the radio button that corresponds to the desired criteria of the ACE in the Source MAC Address field.

- Any — All destination MAC addresses apply to the ACE.
- User Defined — Enter a MAC address and MAC wildcard mask that is to be applied to the ACE in the Destination MAC Address Value and Destination MAC Wildcard Mask fields. Wildcard masks are used to define a range of MAC addresses.
- Any — All source MAC addresses apply to the ACE.
- User Defined — Enter a MAC address and MAC wildcard mask that is to be applied to the ACE in the Destination MAC Address Value and Destination MAC Wildcard Mask fields. Wildcard masks are used to define a range of MAC addresses.

Step 11. Enter a VLAN ID that will be matched with the VLAN tag of the frame.

Step 12. (Optional) To Include 802.1p values in ACE Criteria, check **Include** in the 802.1p field. 802.1p involves the technology Class of Service (CoS). CoS is a 3 bit field in an Ethernet frame that is used to differentiate traffic.

Step 13. If 802.1p values are included, enter the following fields.

- 802.1p Value — Enter the 802.1p value that is to be matched. 802.1p is a specification that gives Layer 2 switches the ability to prioritize traffic and to perform dynamic multicast filtering.
- 802.1p Mask — Enter the wildcard mask of the 802.1p values. This wildcard mask is used to define the range of 802.1p values.

Step 14. Enter the Ethertype of the frame that is to be matched. Ethertype is a two octet field in an Ethernet frame that is used to indicate which protocol is utilized for the payload of the frame.

Step 15. Click **Apply**. The ACE is created. In this example, the created ACE denies traffic that is sent from the defined source MAC addresses to all destination addresses.