Address Resolution Protocol (ARP) Access Control Rules Configuration on 300 Series Managed Switches

Objective

Address Resolution Protocol (ARP) maps the IP address of a device to the MAC address of the same device. ARP inspection is used to protect a network from ARP attacks. When a packet arrives on an interface (port/LAG) that is defined as untrusted, ARP inspection compares the IP address and MAC address of the packet with the IP addresses and MAC addresses previously defined in the ARP access control rules. If the addresses match, the packet is considered valid and is forwarded. This article explains how to create an ARP access control group, how to add rules to an ARP access control group, and how to configure an ARP access control group to a VLAN on the SF/SG 300 Series Managed Switches.

To create protection from ARP attacks, you must follow several steps:

- ARP Inspection must be enabled on the switch. Refer to the article *Address Resolution Protocol (ARP) Inspection Properties Configuration on 300 Series Managed Switches* for help.

- ARP inspection can only be performed on interfaces that are considered untrusted. To configure an interface as trusted or untrusted, refer to the article *Address Resolution Protocol (ARP) Inspection Properties Configuration on 300 Series Managed Switches*.

- Create an ARP access control group. An ARP access control group is a list of the IP address and MAC address of the different devices that are allowed access on an untrusted interface.

- To add additional devices to an ARP access control group, you must then create additional ARP access control rules.

- Assign an ARP access control group to a VLAN. However, you may only configure one ARP access control group per VLAN.

Applicable Devices

- SF/SG 300 Series Managed Switches

Software Version

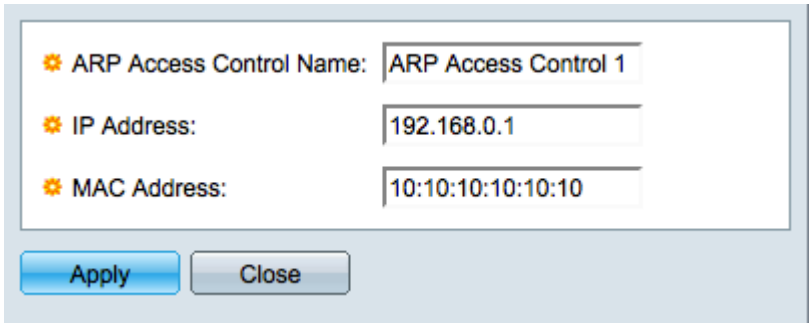
- 1.3.0.62

ARP Access Control Configuration

Create an ARP Access Control Group

Step 1. Log in to the web configuration utility and choose **Security > ARP Inspection > ARP Access Control**. The *ARP Access Control* page opens:

Step 2. Click **Add**. The *Add ARP Access Control* window appears.



Step 3. Enter the desired name for the access control group in the ARP Access Control Name field.

Step 4. Enter the IP address to be assigned to the access control in the IP Address field.

Step 5. Enter the MAC address to be assigned to the access control in the MAC Address field.

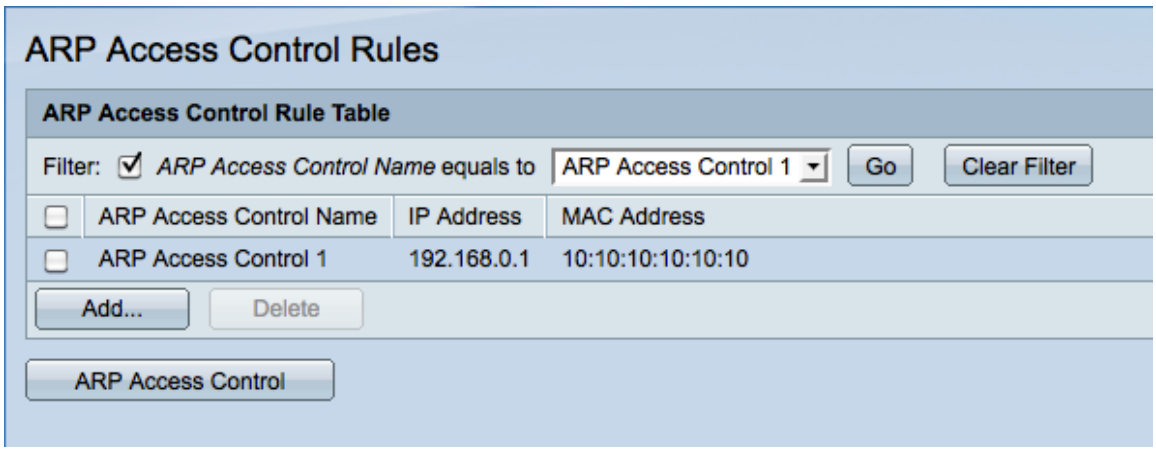
Note: The IP address and MAC address should refer to the same device. This is how the switch verifies that the device is to be trusted.

Step 6. Click **Apply** to apply the changes and then click **Close** to exit the *Add ARP Access Control Name* window.

Add ARP Access Control Rules

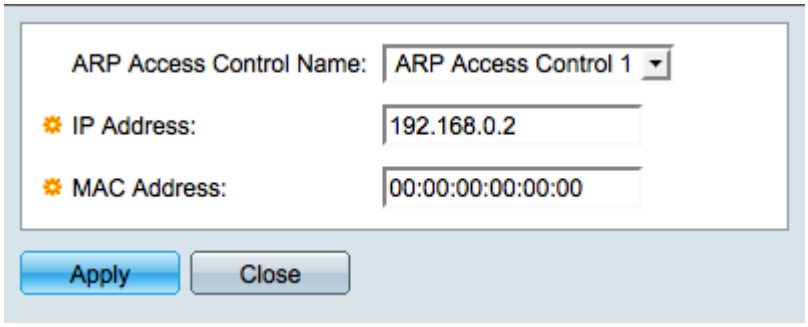
Note: You must have an ARP access control group to add ARP access control rules. Please complete the previous section if you have not done so yet.

Step 1. Log in to the web configuration utility and choose **Security > ARP Inspection > ARP control rules**. The *ARP Access Control Rules* page opens:



Note: If you have many ARP Access Control Names, use the Filter function to filter out the unwanted ARP Access Control Names.

Step 2. Click **Add**. The *Add ARP Access Control Rules* window appears.



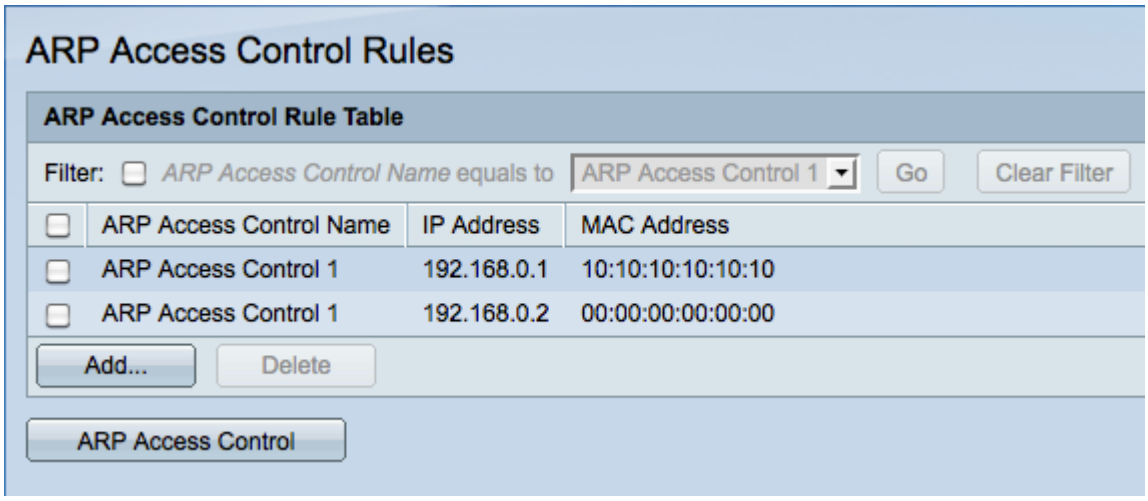
Step 3. Choose an access control name to add another rule to from the ARP Access Control Name drop-down list.

Step 4. Enter the IP address to be assigned to the access control in the IP Address field.

Step 5. Enter the MAC address to be assigned to the access control in the MAC Address field.

Note: The address pair that is entered should be of a new device that you want to add to the access control group.

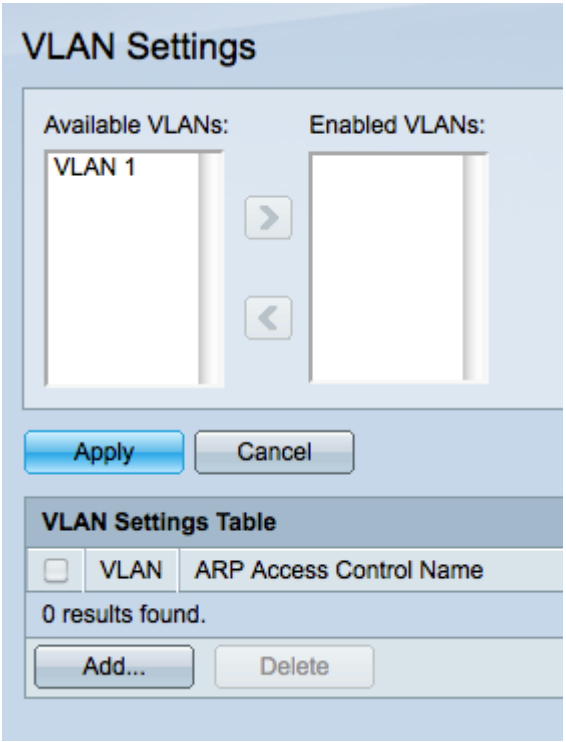
Step 6. Click **Apply** to apply the changes and then click **Close** to exit the *Add ARP Access Control Name* Window.



Configure ARP Access Control to a VLAN

Note: You can only add one ARP Access Control group per VLAN. Use ARP Access Control Rules to add multiple devices to an ARP Access Control group and then configure that group to a VLAN.

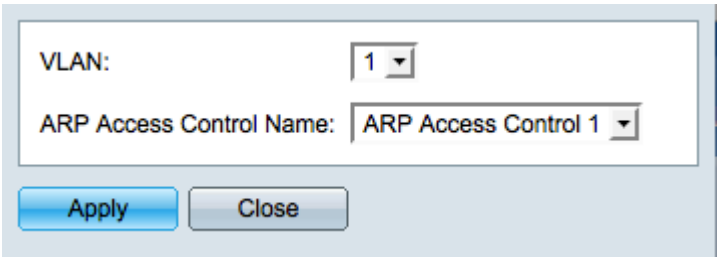
Step 1. Log in to the web configuration utility and choose **Security > ARP Inspection > VLAN Settings**. The *VLAN Settings* page opens:



Step 2. In the Available VLANs field, click the VLAN to which you wish to add an ARP Access Control group and click the **>** button to move it to the Enabled VLANs field.

Step 3. Click **Apply** to enable the VLAN and allow an ARP Access Control to be added.

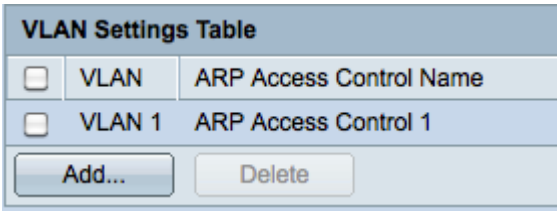
Step 4. Click **Add** to add an ARP Access Control to a VLAN. The *VLAN Settings* window appears.



Step 5. Choose a VLAN from the VLAN drop-down list.

Step 6. Choose the ARP Access Control Name you would like to apply to that VLAN from the ARP Access Control Name drop-down list.

Step 7. Click **Apply** to apply the changes and then click **Close** to exit the *VLAN Settings* window. The VLAN Settings Table should display that the VLAN you chose has the appropriate ARP Access Controls.


VLAN Settings Table
VLAN
ARP Access Control Name
VLAN 1
ARP Access Control 1
Add...
Delete