Simple Network Management Protocol (SNMP) Group Configuration on a 300 Series Managed Switch

Objective

The article explains how to create an Simple Network Management Protocol (SNMP) group on a 300 Series Managed Switch.

Introduction

SNMP is used to manage devices on an IP network. Management Information Bases (MIBs) store information about the switch that can be accessed via SNMP. An SNMP view restricts access to the MIB. Instead of the whole MIB, only part of the MIB is visible. SNMP groups are used to define the read/write privileges of users to different views.

Prerequisites

A few other configurations should be done before this configuration is implemented.

- SNMP is disabled by default and must be turned on before a group can be created. For more details, click here.
- To create a view other than the default, click here.
- After the group is created, you can then assign users to the group. For more information on how to add users to a group, click here.

Applicable Devices

- SF/SG 300 Series Managed Switches

Software Version

- v1.2.7.76

SNMP Group Configuration

Step 1. Log in to the web configuration utility of the 300 series switch and choose **SNMP > Groups**. The *Groups* page opens:

Step 2. Click **Add**. The *Add Group* window opens:

Step 3. Enter a name by which to identify the SNMP group in the *Group Name* field.

Step 4. Click the appropriate SNMP version radio button in the *Security Model* field.

- SNMPv1 and SNMPv2 - Uses community strings to authenticate packets. Since community strings are not encrypted, neither version is secure.
- SNMPv3 - Uses usernames and passwords to authenticate packets along with a host of other security measures not found in versions 1 or 2. SNMPv3 is recommended for its increased security.

Note: Users can only be assigned to a SNMPv3 group. Choose SNMPv3 if you want to later assign users to the group.

Step 5. Check the appropriate security level check box(es) for the SNMP group.

Note: For SNMPv1 and SNMPv2, you may only check No Authentication and No Privacy. For SNMPv3, all three options are available:

- No Authentication and No Privacy - The switch does not authenticate or encrypt the data frames.
- Authentication and No Privacy - The switch authenticates SNMP messages and ensures the SNMP user is an authorized system administrator. No encryption is performed on the message.
- Authentication and Privacy - The switch authenticates the origin of the SNMP message and encrypts the SNMP message.

Step 6. Check the restrictions to associate with the view. These restrictions are applied to

the view (portion of the MIB) that appears in the drop-down list next to the check box. The three options available are:

- Read - Members of the group are only allowed to read the chosen view.
- Write - Members of the group are allowed to write/edit the chosen view.
- Notify - A message is sent to the SNMP user when an event occurs on the chosen view. Notify is only available for SNMPv3.

Step 7. Choose a view from the drop-down list next to the restriction boxes you checked in Step 6.

- Default - Default for read and read/write views.
- DefaultSuper - Default for administrator views.

Note: Additional views are available if you have created them. To create a view, refer to the article *Simple Netowrk Management Protocol (SNMP) Views Configuration on the 300 Series Managed Switches*.

Step 8. Click **Apply** to update the running configuration file and define the new SNMP group. Click **Close** to exit the *Add Group* window.

Step 9. (Optional) To edit a group, check the corresponding check box and click **Edit**.

Step 10. (Optional) To delete a group, check the corresponding check box and click **Delete**.

Conclusion

You have now successfully created an SNMP group on a 300 series managed switch.